The Report of the Special Senate Committee on Security and Intelligence

Chairman
The Honourable William M. Kelly

Deputy Chairman
The Honourable John G. Bryden

January 1999

The Report of the Special Senate Committee on Security and Intelligence

Chairman
The Honourable William M. Kelly

Deputy Chairman
The Honourable John G. Bryden

January 1999

Ce document est disponible en français

Membership of the Committee

The Honourable William M. Kelly, *Chairman*

The Honourable John G. Bryden, *Deputy Chairman*

and

The Honourable Senators:

ANDREYCHUK, Raynell
* CARSTAIRS, Sharon
CORBIN, Eymard G.
LEBRETON, Marjory
* LYNCH-STAUNTON, John
PÉPIN, Lucie
STOLLERY, Peter

**Ex Officio Members*

Original members agreed to by Motion of the Senate:

The Honourable Senators:

Andreychuk, Bryden, Corbin, Fitzpatrick, *Graham (or Carstairs), Kelleher, Kelly, *Lynch-Staunton (or Kinsella, acting) and Stollery.

Other Senators who participated in the work of the Committee:

The Honourable Senator:

Prud'homme.

Orders of Reference

Extract from the *Journals of the Senate* dated Thursday, March 26, 1998:

Resuming debate on the motion, as modified, of the Honourable Senator Kelly, seconded by the Honourable Senator Prud'homme, P.C.:

That, a special committee of the Senate be appointed to hear evidence on and consider matters relating to the threat posed to Canada by terrorism and the counter-terrorism activities of the Government of Canada;

That the Committee examine and report on the current international threat environment with particular reference to terrorism as it relates to Canada;

That the Committee examine and report on the extent to which the recommendations of the Report of the Special Committee on Terrorism and Public Safety (June 1987) and the Report of the Special Committee on Terrorism and Public Safety (June 1989) have been addressed by the Government of Canada;

That the Committee examine and make recommendations with respect to the threat assessment capability of the Government of Canada relative to the threat of terrorism;

That the Committee examine and make recommendations with respect to the leadership role, preparedness and review of those departments and agencies of the Government of Canada with counter-terrorism responsibilities;

That the Committee examine and assess the level of international cooperation between Canada and its allies with respect to the evolving nature of the terrorist threat;

That seven Senators, to be designated at a later date, act as members of the Committee;

That the Committee have power to report from time to time, to send for persons, papers and records, and to print such papers and evidence from day to day as may be ordered by the Committee; and;

That the Committee presents its final report no later than September 29, 1998.

After debate,

The question being put on the motion, as modified, it was adopted.

.....

Extract from the *Journals of the Senate* dated Tuesday, September 29, 1998:

With leave of the Senate,

The Honourable Senator Kelly moved, seconded by the Honourable Senator Carney, P.C.:

That notwithstanding the Order of the Senate adopted on March 26, 1998, the Special Committee of the Senate on Security and Intelligence which was authorised to hear evidence on and consider matters relating to the threat posed to Canada by terrorism and the counter-terrorism activities of the Government of Canada; examine and report on the current international threat environment with particular reference to terrorism as it relates to Canada; examine and report on the extent to which the recommendations of the Report of the Special Committee on terrorism and Public Safety (June 1987) and the Report of the Special Committee on Terrorism and Public Safety (June 1989) have been addressed by the Government of Canada; examine and make recommendations with respect to the threat assessment capacity of the Government of Canada relative to the threats of terrorism; and examine and make recommendations with respect to the leadership role, preparedness and review of those departments and agencies of the Government of Canada with counter-terrorism responsibilities; be empowered to present its final report no later than November 30, 1998; and

That the Committee be permitted, notwithstanding usual practices, to deposit its report with the Clerk of the Senate, if the Senate is not then sitting; and that the report be deemed to have been tabled in the Chamber.

The question being put on the motion, it was adopted.

.....

Extract from the *Journals of the Senate* dated Thursday, November 19, 1998:

With leave of the Senate,

The Honourable Senator Kelly moved, seconded by the Honourable Senator Kinsella:

That notwithstanding the Order of the Senate adopted on September 29, 1998, the Special Committee of the Senate on Security and Intelligence be empowered to present its final report no later than December 17, 1998.

The question being put on the motion, it was adopted.

.....

Extract from the *Journals of the Senate* dated Tuesday, December 1, 1998:

With leave of the Senate,

The Honourable Senator Kelly moved, seconded by the Honourable Senator Kinsella:

That notwithstanding the Order of the Senae adopted on November 19, 1998, the Special Committee of the Senate on Security andn Intelligence be empowered to present its final report no later than Friday, January 15, 1999.

After debate,

The question being put on the motion, it was adopted.

.....

Extract from the *Journals of the Senate* dated Tuesday, December 8, 1998:

With leave of the Senate,

The Honourable Senator Kelly moved, seconded by the Honourable Senator Rivest:

That the Special Senate Committee on Security and Intelligence be permitted, notwithstanding usual practices, to deposit its Report on the examination of the current international threat environment with particular reference to terrorism as it relates to Canada with the Clerk of the Senate if the Senate is not sitting; and that the Report be deemed to have been tabled in the Chamber; and

That, if before the prorogation of the present session of Parliament, the Special Senate Committee on Security and Intelligence has adopted but not tabled its Report, the Honourable Senators authorized to act for and on behalf of the Senate in all matters relating to internal economy of the Senate during any period between sessions of Parliament, be authorized to publish and distribute the Report of the Committee

The question being put on the motion, it was adopted.

Paul Bélisle
Clerk of the Senate

TABLE OF CONTENTS

FOREWORD

Over the past 15 years, three Special Committees of the Senate have been convened to examine aspects of the federal government's security and intelligence community. The first Senate Special Committee on Terrorism and Public Safety was reported in June of 1987, and the second Senate Special Committee on Terrorism and Public Safety was reported in July of 1989.

The first two Committees convened after the occurrence of terrorist incidents in Canada. Although no actual incident acted as a catalyst for this Committee, the objective of all three Commitees was the same – namely, to ensure that our security and intelligence organizations are staying ahead of events, and not simply reacting to them. With changes in the geopolitical environment and advances in technology, this challenge has become increasingly daunting.

It is fair to say that the undercurrent of the previous Commitees' reports was one of concern that we were perhaps overly complacent, and hence were not effectively grappling with the terrorist threat, and we were not as prepared as we should have been to respond to an actual incident.

The theme of this Report is very different. There has been a positive change in the level of preparedness and professionalism in the security and intelligence community. Issues and concern identified by the previous Committees have been, in the main, addressed. However, the threat environment has changed considerably over the past decade and new challenges now face our security and intelligence community. As discussed in this Report, technological advances pose the most serious challenge, and may place our security and intelligence organizations on a "technological treadmill" in order to maintain our preparedness.

There have been comments in the media and elsewhere about this Committee and the previous Committees' decision to hold hearings *in camera*. On one hand, public hearings would probably have contributed to public understanding and transparency of security and intelligence matters and would also contribute to public confidence in our security and intelligence institutions. On the other hand, the Committees concluded that *in camera* sessions would encourage witness candour. In fact, a few witnesses insisted on giving their evidence *in camera*. Furthermore, the Committees were concerned that public hearings might result in the sensationalizing of particular testimony.

It has been my honour to chair this Committee and the previous two. I have been privileged to witness the very substantial progress of our security and intelligence community. I wish to recognize the many men and women in that community for their professionalism, and for their dedication and work for the security of Canada. I should like, in particular, to recognize several officials who gave unstintingly of their time to this Committee: John Tait, the Coordinator, Security and Intelligence, in the Privy Council Office; Ward Elcock, Director, Canadian Security Intelligence Service; Jean Fournier, Deputy Solicitor General, and Commissioner Philip Murray of the Royal

Canadian Mounted Police.

Of particular concern is the current extent of personnel turnover at senior levels in the community. Several officials who appeared before this Committee whom I would number among the 'best and brightest' have, within a very short time, left the community.

I wish to record the Committee's appreciation to all witnesses who appeared before the Committee, some of whom appeared on multiple occasions. We are also grateful to our Clerks: Nadine S. Huggins and Barbara Reynolds; our Legislative Clerk, Till Heyde; as well as Don Gracey, Adele Pellegrino and the rest of the CG Management and Communications team. Thank you to CG Management and Communications for identifying witnesses, resource persons and preparing multiple drafts of the Committee Report. The contribution of our French editor, Louis Majeau, and our translators are also reflected in the text. Grateful mention must also be made of the hardworking interpreters, console operators, transcribers and staff of the publications service who provided service to the Committee.

In preparing this Report, the Committee gave particular attention to the question of threat assessment and analysis, in order to satisfy itself that mechanisms are in place to identify situations which put Canada and Canadians at risk.

This brings me to my final point. Advances in technology give us increasingly effective tools to monitor terrorists and interdict their criminal actions. Those same advances in technology give our security and intelligence organizations unprecedented ability to interfere with the personal rights and freedoms of Canadians. The Committee received no evidence that our security and intelligence community acts illegally or unconstitutionally. However, the presence of those abilities will always be a temptation, or create public unease or suspicion. One of the objectives of this Committee, therefore, was to consider the need for enhanced review mechanisms to guard against the abuse or excessive use of power and to give the public as much confidence as possible in this regard.

I wish to thank my fellow Committee members. Committee reports by their nature reflect a consensus of views. It will come as no surprise to anyone that this Committee had a divergence of views on several matters, and those divergences were subordinated to the need to achieve a consensus. I look forward to the debate in the Senate Chamber on this Report where, I trust, Committee members will bring their individual perspectives to the very important, complicated and sensitive matters canvassed in this Report.

William M. Kelly
Chairman

On March 26, 1998, the Senate approved an Order of Reference to constitute a Special Committee on Security and Intelligence. In essence, the Committee's mandate was to pick up from where the previous Senate Special Committees on Terrorism and Public Safety had left off. Those Committees reported in June 1987 and in May 1989.

The Special Committee on Security and Intelligence conducted hearings from May 26, through to November 5, 1998.

Prior to the commencement of formal hearings, the Chairman and Committee staff made contact with a wide range of experts and commentators on the subject of terrorism, security and intelligence in order to identify the issues and refine the Committee's approach to its examination. These contacts included foreign and Canadian government officials, Canadian and foreign security intelligence officials, federal, provincial and municipal law enforcement officials, academics, representatives of ethno-cultural groups and research organizations.

Structure of Hearings

Before hearings began the Committee made the decision that all hearings would be *in camera*. This decision was made in order to encourage the maximum possible candour from witnesses to avoid the possibility that a particular statement by a witness might be sensationalized and to ensure security is not compromised in any way. A few private witnesses either stated their clear preference for *in camera* hearings, or agreed to appear only *in camera*.

Hearings were attended only by Senators and staff of the Committee, Senate staff and staff of individual Senators. Transcripts of hearings were made, but were not released to the public.

Witnesses appeared before the Committee by invitation only. An invitation to appear before the Committee was, however, extended to any individual, group or organization who requested to appear. Invitations to appear before or make submissions to the Committee were sent to all non-government groups, organizations or individuals who appeared before either of the previous Senate Special Committees on Terrorism and Public Safety.

Listed at Appendix A are the witnesses who appeared before the Committee and their affiliations. A total of 97 witnesses appeared. Committee staff interviewed an additional 42 persons. A list of those persons is included in this Report as Appendix B.

The Committee is grateful to all those witnesses who took time to appear before the Committee in some cases appearing multiple times and to those who made written submissions to the Committee.

The Committee's hearings were divided into four groups or modules addressing the following topics:

- The current risk assessment and changes in the security and intelligence environment since the last Special Committee on Terrorism and Public Safety.
- Responses to the recommendations and observations of the two previous Special Committees on Terrorism and Public Safety.
- Emerging Issues.
- A review of leadership, coordination, review and oversight of the security and intelligence community.

Orientation of the Report

The reports of the two previous Special Committees on Terrorism and Public Safety were well-received and reviewed by authorities, because they went to unprecedented lengths to identify the government organizations that played a role in counter-terrorism and to describe their functions and inter-relationships. The reports also tried to be as candid as possible in describing the issues the Committees came upon. The Committees did so in order to help demystify such organizations, to contribute to public awareness about their existence and also to contribute to a public discussion of the issues surrounding Canada's counter-terrorism initiatives.

This Report endeavours to continue that tradition in order to bring more information to the public. The Committee hopes to encourage a better understanding and public discussion of the issues involved, many of which are highly complex with no simple or readily-apparent solutions.

Obviously, some information disclosed to the Committee during *in camera* hearings is not revealed in this Report. Information was not included in this Report if the Committee concluded that its release could reasonably be expected to undermine Canada's security. There are certain matters that the Committee has decided should be kept confidential. Such matters have been addressed in a letter to the Prime Minister, with copies to the individual ministers concerned.

Structure of Report

Each chapter of the Report begins with a summary of the major observations and recommendations of the Committee pertaining to the subject-matter of that chapter. A more detailed discussion and analysis follows in each chapter.

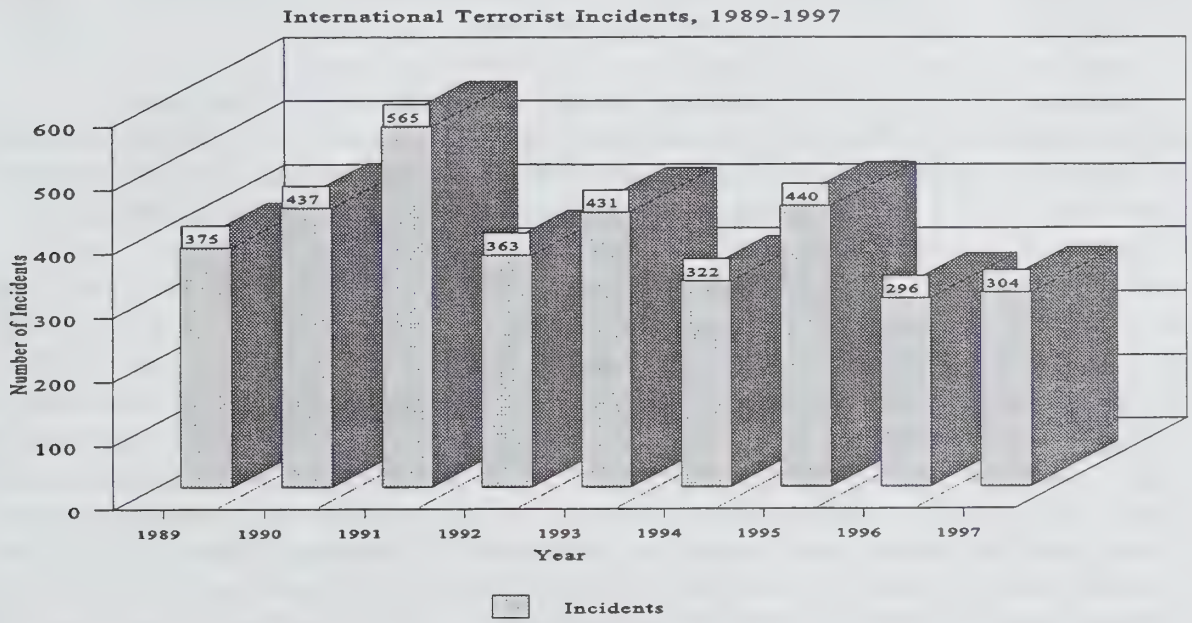
CHAPTER I

THE CURRENT SECURITY AND INTELLIGENCE ENVIRONMENT AND A CURRENT ASSESSMENT OF RISKS TO CANADA'S SECURITY

Overview

Since the Senate Special Committee on Terrorism and Public Safety reported in 1989, much has changed in terms of the extent and nature of the security threats facing the world. **Figure 1** illustrates the number of terrorist incidents world-wide since 1989. It is important to consider this figure in the context of the unknown number of terrorist incidents that may have been aborted, or otherwise never came to fruition, because of counter-terrorism actions by police and security intelligence agencies.[1]

Figure 1



Note: Data from the United States Department of State.

Overall, Canada and Canadians are not a major target for terrorist attacks. Canada remains, however, a "venue of opportunity" for terrorist groups: a place where they may raise funds, purchase arms and conduct other activities to support their organizations and their terrorist activities elsewhere. Most

[1] For example, the attempted bombings of the Holland Tunnel and the United Nations buildings in New York.

of the major international terrorist organizations have a presence in Canada. Our geographic location also makes Canada a favourite conduit for terrorists wishing to enter the United States, which remains the principal target for terrorist attacks world-wide. In 1997, over one-third of all terrorist attacks were against United States targets.

Testimony by witnesses indicates that the number of terrorist incidents in Canada has declined. This is consistent with the international trends in terrorism. In 1997, world-wide, there were 304 terrorist attacks, one of the lowest totals recorded since 1971.[2] While this trend is clearly encouraging, the Committee notes that a single terrorist incident of the magnitude of the bombings of Air India flight 182 or Oklahoma City is cataclysmic. Furthermore, the Canadian Department of Foreign Affairs and International Trade employs 1,212 Canadian and 4,288 local employees at our missions abroad; 1.5 million Canadians live outside Canada on a semi-permanent basis and up to four million Canadians travel abroad each year. Canadians also visit areas of political instability with increasing frequency.[3] Canadians thus can become innocent and unintended victims of terrorism. Sixty Canadians were on an EgyptAir flight hi-jacked at Luxor (1996). Four Canadians were kidnapped in Colombia (1996-1997), one in Yemen (1993-1994) and one in Chechnya (1998). Three Canadian tourists were kidnapped by Rwandan rebels in The Congo (1998) and several local employees of the Canadian High Commissions were injured in the bombings of the United States embassies in Nairobi and Dar-es-Salaam (1998). As the previous Senate Special Committees on Terrorism and Public Safety noted, there is no ground for complacency.

The previous Senate Special Committees on Terrorism and Public Safety noted that as countries upgrade their defences against terrorism ("hardening targets"), terrorist groups tend to seek out other countries or targets that remain relatively soft. The bombings of the United States' embassies in Nairobi and Dar-es-Salaam and the bombing in Omagh, Northern Ireland are illustrations of terrorists seeking out softer targets. The designation of 30 groups as "Foreign Terrorist Organizations" by the United States under the *Antiterrorism and Effective Death Penalty Act, 1996* may, as it is intended to do, encourage terrorists to mount actions other than in or against the United States. Hardening of targets means that civilians and countries with a low previous incidence of terrorism may increasingly be targets. Deportation of known or suspected terrorists, Canada's role in peacekeeping and peacemaking missions, our role in mediating terrorist hostage-takings[4], the presence in Canada of a large number of foreign diplomatic and other facilities, the fact that we are largely a nation of immigrants, the fact that Canada is often a venue for international summits and other events and our continuing role in world affairs mean Canada cannot presume to be immune from terrorism. These situations are taken seriously by Canada's security and intelligence community, but considerable complacency ("it can't happen here") persists among the public-at-large.

---

[2] United States State Department figures (April, 1998).

[3] Figures from the Department of Foreign Affairs and International Trade.

[4] For example, the Canadian Ambassador's role in trying to resolve the MRTA's (Tupac Amaru Revolutionary Movement's) occupation of the Japanese Embassy in Lima, Peru, 1997.

It is the Committee's wish to ensure that the Canadian government is not simply reacting to events, but is also planning sufficiently ahead to minimize the number and impact of terrorist incidents. A proper analysis of the government's counter-terrorism capability must include not only the government's ability to respond effectively to a terrorist incident and the current situation, but must also include sufficient forward thinking to be able to identify and counter future situations.

Definitions and the Scope of the Committee's Review

The first Senate Special Committee on Terrorism and Public Safety grappled at length with finding a definition of terrorism that reflects the current environment.[5] The term "terrorisme" appears to have originated from the phrase "régime de la terreur" coined by Robespierre during the French Revolution. The term was anglicized by Edmund Burke who railed against the excesses of that Revolution.[6] The first Senate Special Committee on Terrorism and Public Safety found, at the time, some 109 definitions of "terrorism".

How "terrorism" is defined has changed dramatically in response to the ebbs and flows of domestic and international politics over the centuries. From its revolutionary origins, terrorism has been variously defined as, or equated with, popular revolutionary movements, mass repression practised by totalitarian states, anti-colonialist or nationalist insurrections, separatist movements, or low intensity warfare mounted or supported by renegade states. Historically, terrorism has been equated with violence or at least the threat of violence. In his attempt to find a workable and accepted definition of terrorism, Schmid studied the common elements of 109 definitions and found a reference to "force" or "violence" in 83.5%. References to political motivations came next at 65%.[7] Subsection 2(c) of the Canadian Security Intelligence Service Act, which although not referring to terrorism by name is usually taken to cover it, also refers to:

> "*activities...directed toward or in support of the threat or use of acts of* ***serious violence*** *against persons or property for the purpose of achieving a* ***political objective*** *within Canada or a foreign state, ...*"[8]
> (emphasis added)

---

[5] See **Report of the Senate Special Committee on Terrorism and Public Safety** (June, 1987), Supply and Services Canada, p.p. 1-4.

[6] For an extensive review of the origins of the word "terrorism" and a discussion of the evolution of the term see Bruce Hoffman, **Inside Terrorism**, Victor Gollanz, London: Wellington House, 1998, Chapter I.

[7] Alex P. Schmid, et al, **Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature**, Transaction Books (1988), p.p. 1-9.

[8] One of the issues raised by this definition is: Why limit the scope of violence to "serious" violence; what constitutes "serious" violence; and who decides? The draft Ontario Counter-Terrorism Plan adds further complications by referring to "extraordinary violence" in its definition of "terrorist activity".

International conventions relating to terrorism, the United States Antiterrorism and Effective Death Penalty Act, definitions used by the Federal Bureau of Investigation and the United States Department of Defence also have references to force, violence or the threat thereof as the common thread.

It is perhaps time that such definitions of terrorism be rethought. As will be discussed later in this Chapter, the modern terrorist has access to tactics that would not be generally understood as "violence" or "force", but can be equally devastating. For example, information warfare and cyber terrorism do not fit comfortably into existing definitions that revolve around violence or the threat of violence. Furthermore, it is no longer necessarily the case that terrorist attacks are oriented towards communicating a political message or gaining allegiance to a political organization or cause. In recent incidents, retribution for perceived past wrongs, or destabilization appear to be the objective.

In 1991, French criminologist Xavier Raufer advanced the concept of the "gray area phenomenon" to try to accommodate the evolution, combinations and permutations of terrorism now extant in the world. Terrorism became more broadly defined by Raufer and his adherents as any threat to the stability of states posed by non-state and non-government actors or organizations.

Another issue that bedevils the search for a workable definition of terrorism is the distinction between terrorism and criminality, especially in today's world of "narco-terrorism" and transnational crime. As was the case with the previous Senate Committees on Terrorism and Public Safety, the Committee asserts that terrorism is crime and should be treated as such. Terrorism is, however, a particular type or subset of crime, distinguished from other types of crime by the motivations of the perpetrators. While both use criminal (and often identical) means, terrorists are motivated by a "cause". Other criminals are motivated by the prospect of personal or organizational economic aggrandizement. The "causes" advanced by terrorism include political or ideological objectives, religion, nationalism, ethnic separation, or any combination thereof.

Within the generic definition of terrorism are several subsets:

State-Sponsored Terrorism has never constituted a significant direct threat to Canada. States that fund, train, provide a haven for, or otherwise promote terrorism include Iran, Iraq, Syria, Sudan, Libya and regimes such as the Taliban in Afghanistan[9]. States sponsor terrorism as a cost-effective method of advancing their interests and, in some cases, as a cost-effective alternative to conventional warfare. State-sponsored terrorism continues to be a major threat to nations such as the United States. State-sponsored terrorism is, under subsection 2(c) of the Canadian Security Intelligence Service Act, a threat to the security of Canada even if Canada is used only as a base to support such terrorism directed at other countries.

Agitational or Insurgent Terrorism springs from non-state, but usually highly organized, groups. Such groups may have originated from guerilla organizations in some area of the world. Agitational or insurgent terrorist groups are usually transnational organizations with their own command

[9] **Patterns of Global Terrorism**, United States Department of State, April 1998. p.p. 29-33.

structures, funding networks and training facilities. They are often affiliated with one or more "legitimate" political or benevolent organizations that act as their fundraising, propaganda or political lobbying wings. Because of their transnational structure, such groups are able to undertake legal actions in one or more countries in support of illegal activities elsewhere.

Loosely Affiliated Terrorists have been responsible for the bombing of the World Trade Centre and the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Historically, in order to frustrate detection some terrorist groups organized their activists into small cells. However, those cells were usually connected to a command structure that exercised some control and coordination over the cells' activities. The phenomenon of completely autonomous individuals or terrorist cells represents a new and major type of threat. The common motivator could be a charismatic leader, religion, ideology or some Patriot Militia ideology or Millennialist philosophy. This type of terrorism constitutes a particular threat because there is no organization or defined command structure that can be infiltrated, the affiliations are often temporary and their ad hoc nature makes them very unpredictable.

Terrorism for Hire is a permutation or combination of the foregoing types of terrorism, also sometimes referred to a "subcontracting terror". Muammar Qadhafi is reputed to have pioneered this tactic when he hired the Red Army to carry out terrorist attacks on behalf of Libya in the early 1980's.

There is a range of groups often classified, or referred to, as "terrorist" that do not fit comfortably within the framework adopted by the Committee. Such groups are not motivated by a cause per se nor do they constitute a realistic threat to the security of Canada or to any other state. Such groups include the complex of hate groups, skinheads and various Millennial groups.

The previous Senate Special Committees on Terrorism and Public Safety included militant First Nations organizations, such as the Mohawk Warriors, within the typology of terrorism. In testimony before the Committee, law enforcement and security intelligence personnel expressed their view that most persons within such groups are motivated by the prospect of personal gain. They have no political or ideological motivations other than as a cover for their criminal activities. The Committee has, therefore, excluded such groups from this review. In doing so, however, neither the Committee nor the security intelligence community down-plays such groups or persons within them as threats to law and order, or even as threats or potential threats to the security of Canada.

Keeping Track of Terrorism

There does not appear to be a reliable list of terrorist incidents in Canada. The Committee understands that a list was maintained until some time in 1992. The project did not continue thereafter. The Department of Foreign Affairs and International Trade did provide the Committee with a list covering the period 1994 to October 1998. That list included 17 terrorist incidents outside of Canada affecting Canadians. Foreign Affairs warned that the list should not be considered in any way as definitive.

The absence of a list makes it difficult to make an objective assessment of the threat environment and of the performance of the security and intelligence community. The Committee feels it worthwhile, therefore, to expend the resources necessary to maintain a list of terrorist incidents in Canada and affecting Canadians or Canadian interests abroad. This function should logically be coordinated by the Privy Council Office since the necessary information would come from several sources within the government.

The Current Environment

The international security environment has changed considerably since 1989. The major environmental changes are summarized in this Chapter. The Committee does not imply that all of these environmental changes impact on Canada. Some or all do apply to the United States and to other of Canada's allies, however. They are, therefore, important considerations for Canada's security intelligence community, not only for our own purposes, but also in our role as part of the common international front against terrorism.

The Geopolitical Environment: We no longer face a bipolar world, divided between the Soviet Bloc and its allies and the Western bloc revolving around the United States. Since the collapse of the Union of Soviet Socialist Republics, the United States is the only *bona fide* world power. This situation may, however, be temporary as the Peoples' Republic of China evidently aims to become a superpower of at least equivalent stature to the United States, perhaps as early as the end of the first decade of the 21st Century.

The end of bipolar geopolitical competition has reduced state-sponsored terrorism by the Soviet Bloc. Neither Russia, nor any other country of the former Soviet Union, has the resources to fund a wide range of terrorist groups and activities.[10] Nor is the Soviet Bloc any longer an important training ground for terrorists, or a haven for terrorists on the run. The current leadership in Moscow appears to recognize that the disintegration of the Union of Soviet Socialist Republic and the economic and political instability in the region have left something of a geopolitical vacuum. A terrorist action traced to Russia could well cause retaliation against Russia. Furthermore, a terrorist threat or incident affecting United States' interests could invite United States intervention in a region or state close to Russia or of strategic importance to Russia. In its current condition, Russia would be hard-pressed to protect its interests. In a unipolar world, terrorism has risks of setting off a chain reaction of unintended and unforeseen consequences that, for all but renegade states, usually outweigh any reward.

---

[10] This is not to say that terrorism does not exist in the countries of the former Soviet Union. Domestic terrorism, with a strong organized crime component (Russian Mafia) appears to be increasing dramatically. Some domestic terrorist groups such as the Czechnian rebels (depending on one's perspective and definition of terrorism) also have state, or quasi-state, support. The Confederation of Independent States (CIS) has also expressed concerns about the activities of terrorist organizations in member states or on their borders. For example, the religious fundamentalist Wahhabites are accused of destabilizing Uzbekistan and of being sponsored by Afghanistan.

With the collapse of the Soviet Union, the decline of the Soviet Bloc-sponsored terrorism has changed the nature of the terrorist threat, but has not materially reduced it. A number of terrorist groups has had to find new sponsors. "The numerous poisonous snakes of the new international order may well turn out to be as dangerous as the old Soviet dragon".[11]

The "Criminalization" of Terrorism: In its reports, the previous Senate Special Committees on Terrorism and Public Safety commented on the growth of "narco-terrorism": alliances between terrorist groups and the drug cartels. Into this partnership the terrorist organizations bring their para-military skills and organization to protect the drug operations and intimidate interfering governments. For their part, the drug cartels give the terrorist organizations access to vast sums of money from drug profits, far in excess of anything the terrorist organizations could raise through traditional means. The drug cartels also educated the terrorist organizations in the transfer and laundering of money. Today, almost all the major insurgent groups engage in drug trafficking as a method of fundraising. Colombia's FARC, Peru's Sandaro Luminoso, Mynamar's Khun Sa Militia, Turkey's Kurdistan Workers' Party (PKK), the Liberation Tigers of Tamil Eelam (LTTE) and Afghanistan's Hizbi-Islami are examples of terrorist groups that engage in drug trafficking, either on their own or in partnership with drug cartels. These activities are international in scope, but may occur in Canada as well. Drug money gives such groups access to wealth upon which sophisticated, world-wide organizations can be built to continue their insurgent or terrorist activities, regardless of the support in the homeland for those activities and regardless of the success of the insurgent activities in the field. For fundraising purposes, terrorist organizations often engage in criminal activities such as extortion, theft, bank fraud and money laundering. Many terrorist organizations engage in gun-running and smuggling, including smuggling illegal aliens.

Some witnesses before the Committee expressed concern about an apparent new trend for major international terrorist groups, namely the metamorphosis of some into full-blown criminal organizations. This may particularly be the case with insurgent terrorist groups. The political objectives that originally motivated such groups have been subordinated or completely lost to the attractions of the vast personal wealth that can be generated by criminal activities. Because some such groups began as paramilitary organizations with some of their members having combat training and experience, they pose a particular threat as criminal organizations. Royal Canadian Mounted Police witnesses discounted this as a significant current or direct threat to Canada. The trend bears watching in Canada nonetheless.

One might assume, furthermore, that the final phase in the evolution of such groups will be their active involvement in legitimate commercial enterprises as a cover for their criminal activities. In doing so they would follow the precedent established by La Cosa Nostra, the Russian Mafia and other organized crime groups. The Liberation Tigers of Tamil Eelam, for example, are alleged to have invested heavily in the stock and money markets, in real estate, finance companies, farms,

---

[11] R. James Woolsley, Director, United States Central Intelligence, quoted in **The Economist**, "Indiana Jim and the Temple of Spooks", March 20, 1993, p. 34.

video rental shops and in restaurants;[12] anything, in fact, that is highly profitable and gives access to pools of cash. The Liberation Tigers of Tamil Eelam and the Irish Republican Army are said to own and operate fleets of deep-sea ships and, in addition to guns and other contraband cargo, carry fertilizer, timber, sugar, cement and other commercial goods for legitimate (and one assumes innocent) clients. Terrorist organizations that reinvent themselves as multinational commercial enterprises will present substantially greater challenges to those with responsibility for law enforcement and the protection of national and international security.

The Fiscal Environment: Since 1990, governments of all developed countries have embarked on aggressive cost-cutting and fiscal restraint. In Canada, operating funding for federal government agencies with a security or intelligence role fell from $463.9 million in fiscal year 1989-90 to $333.1 million in fiscal year 1997-98. Funding for the Canadian Security Intelligence Service, Canada's principal security intelligence agency, fell from $179.4 million in 1990-91 to $167.6 million in 1997-98. (See **Table 1**).[13]

Table 1

ESTIMATE OF CANADIAN SECURITY AND INTELLIGENCE COMMUNITY

	1990-91 (1)	1990-91 FTE's (1)	1998-99	1998-99	$ Decrease	$ % Decrease	$ % (2) Decrease in constant $	FTE % Decrease
Total (3)	$463,884,002	5,440.6	$333,076,103	4,398.1	$130,807,899	28.2	40.5	19.2
CSIS	$205,000,000	2,680.0	$153,891,000	2,000.0	$51,109,000	24.9	41.3	25.4
CSE	$105,109,000	892.0	$104,993,000	887.0	$116,000	0.1	16.9	0.6

Figures supplied by the Office of the Auditor General. Constant dollars are dollars adjusted for inflation for comparison purposes. This is in constant 1995/96 $ assuming a 2% inflation rate each year. ***Includes*** *the intelligence components of the Department of National Defence, Foreign Affairs,*

[12] Rahan Gunaratna, **International and Regional Security Implications of the Sri Lankan Tamil Insurgency**, Alumni Association of the Bandaranake Centre for International Studies and the International Foundation of Sri Lankans, London, England, (1997) p.24 and interview with Dr. Peter Chalk on July 9, 1998.

[13] Figures assembled for the Committee by the Privy Council Office. The figures are approximations since there is no global or centralized budget for the security and intelligence sector (See Chapter IV). The Auditor General of Canada calculated total expenditures in the "intelligence community" as some $440 million in 1995-96. See **Annual Report to the House of Commons Auditor General of Canada**, Chapter 27, (November, 1996).

the Solicitor General, the CSIS, CSE, Privy Council Office (intelligence assessment; policy), the Security Intelligence Review Committee, the Inspector General for CSIS, and the Commissioner for CSE. ***Excludes*** *the security and intelligence components of the RCMP, Transport Canada, Citizenship and Immigration, Revenue Canada, and other federal departments/agencies. CSE's 1998/99 figures include additional funding for the CSE Commissioner's Office, which was established in June 1996.*

Funding constraints have forced our security intelligence organizations to become more efficient, rely more on partnerships and shared intelligence and to find innovative ways of achieving their mandates. In its response to the Auditor General's 1996 review of control and accountability in the Canadian intelligence community, the intelligence community responded, in part, as follows:

> "*... the Canadian intelligence community has more consumers interested in more topics, while at the same time it has fewer resources to do the job.*" [14]

The resources situation will become particularly acute as the Canadian Security Intelligence Service and other organizations within the federal intelligence community grapple with technological advances, particularly advances in encryption, global satellite technology and with economic espionage. The Committee notes, in this regard, that next year's budget for the United States' security and intelligence sector has been increased by approximately two billion dollars (USD). The amount of the increase alone is more than four times the total current budget for Canada's security intelligence community.

Failed States: Failed states are nations that disintegrate as viable political and constitutional entities, or where governments lose their legitimacy to the extent of being unable to retain public order. In modern times, states have often failed due to economic, fiscal, environmental or other problems that in turn, sometimes prompt internal ethnic or religious conflicts. Failing states often generate emigration. Security threats occur if the militant fringe of the emigré community endeavours to replicate or support the homeland dispute in their new country.

One benefit of the Cold War and the bipolar geopolitical world was that superpower influence acted as a check against state failures, at least against the failure of those states within the United States' or the Soviet Union's respective spheres of influence. The end of the Cold War contributed to a number of state failures. Future failures are predicted to be predominantly in eastern Europe, Asia and Africa.[15]

---

[14] Ibid. p. 27-28.

[15] Interview with Dr David Dewitt, Director, Centre for International and Strategic Studies, York University, (May 13, 1998). Chadwick F. Agler, "Failed States and the Failure of States: Self Determination, States, Nations and Global Governance"; Daniel Esty, Jack Goldstone, Robert Ted Gurr, Pamela Surko, Alan Unger and Robert Chen, "The State Failure Project: Early Warning Research for

Religious Extremism: [*The Committee wishes to emphasize to readers of the following section that the Committee is not claiming that any religion, including religious fundamentalism, is a source or motivator of terrorism. The Committee acknowledges that most religions and the vast majority of religious adherents abhor violence and do not knowingly support or condone terrorism. It is a fact of life, however, that some organizations, operating under the guise of religion, advocate, or engage in violence.*]

Historically, a number of terrorist organizations had, or at least claimed, a religious association. Examples from history include various Jewish organizations agitating against Britain for independence, the Muslim dominated FLN in Algeria, the Catholic Irish Republican Army, the Protestant Ulster Freedom Fighters and the Ulster Volunteer Force and the predominantly Muslim Palestinian Liberation Organization. Such groups espoused religion as a common denominator, but pursued essentially nationalist objectives.

The fall of the Shah of Iran and the conversion of Iran to an Islamic republic in 1979 marked a new and important trend wherein religion was represented by militant extremists as their sole motivation for terrorist actions. Such groups fell comfortably into the conventional definition of terrorism because their targets were "political", namely governments of the Western alliance, in particular the government of the United States and its policies. Since then terrorism ostensibly motivated by religion has grown as a force to be reckoned with. According to some experts, groups representing themselves as motivated by religion now account for nearly half of all known active international terrorist groups. Furthermore, such terrorists appear to have a different value system from traditional terrorist groups and appear less concerned about causing high civilian casualties in a terrorist action. Traditionally, terrorist groups eschewed mass slaughter lest it prompt abhorrence of the groups and rejection of their aims.

Terrorism by those claiming a religious motivation varies significantly from conventional terrorism in another way. Whereas conventional terrorist groups tend to have defined organizational structures and organizational allegiances, militants claiming a religious cause often gravitate to small cells of people held together by personal or spiritual bonds. This makes the latter more difficult to infiltrate, monitor and interdict; they are, in effect, multi-headed hydras.

Competition and Convergence: In the telecommunications and information technology fields there has been an almost exponential growth in the number of suppliers and in the services being offered. One telephone call can now involve multiple carriers: the company that provides the cordless connection, the facilities-based carrier that operates the Public Switched Telephone Network (PSTN), the reseller that carries the call to another Public Switched Telephone Network

---

the United States Foreign Policy Planning"; Michael Nicholson "Failed States, Failing Systems"; papers presented at **The Conference for Failed States and International Security: Causes, Prospects, and Consequences**. Purdue University, West Lafayette. February 25-27, 1998. Robert Kaplan, "The Coming Anarchy". **The Atlantic Monthly**, 273, No. 2 (February 1994), p.p. 44-76.

and the local reseller that carries the call to its final destination. There have also been substantial cross-overs between industry sectors in providing services. For example, cable and telephone companies are beginning to offer the same services. In 1989, when the last Special Committee on Terrorism and Public Safety reported, each province had essentially one telecommunications provider. Now there are multiple facilities-based and resale telecommunications providers offering a range of competitive products. Telecommunications and information technologies are important tools for terrorists. Competition and convergence have resulted in a variegated industry structure that challenges security intelligence agencies in conducting lawful monitoring and interception.

Deregulation and Privatization: There has been a sea of change in public policy that since 1987 has led to the privatization by government of many of its assets and operations and the deregulation (or the exercise of regulatory forbearance) in many sectors under the regulatory jurisdiction of government. Of particular relevance to the Committee has been airport privatization that has changed the structure of airport management, including the management of airport security; and the deregulation of telecommunications that has resulted in a virtual explosion of the number of telecommunications companies and the services offered.

The Tactics of Terrorism

When the Senate Special Committees on Terrorism and Public Safety conducted their reviews, the principal tactics or tools used by terrorists were assassinations, conventional bombings, aircraft hi-jackings and kidnappings. These are still the tactics to which today's terrorists usually resort and, in 1997, the predominant type of terrorist attack was bombing.[16] However, a number of new and potentially more devastatingly effective tools have been added to the terrorists' arsenal.

Weapons of Mass Destruction (WMD): When the last Senate Committee on Terrorism and Public Safety reported in 1989, conventional wisdom at that time held that terrorists were unlikely to engage in actions that would result in large civilian casualties or other collateral damage. The theory was that terrorists would eschew such actions lest they inspire public revulsion and antipathy to the terrorist organization and its cause.

Since then, there has been a number of terrorist incidents aimed at maximizing civilian casualties. The Aum Shinrikyo[17] cult's release of Sarin gas in the Tokyo subway system may well have let the "genie out of the bottle" in terms of terrorist groups using weapons of mass destruction in order to heighten the impact.

Anecdotal evidence indicates that fissionable materials, military and industrial grade plutonium and even nuclear weapons have leaked out of the former Soviet arsenal and may be in the hands of, or accessible to, terrorist groups. Perhaps the most worrisome consideration is that a few renegade

---

[16] United States Department of State figures.

[17] Aum Shinrikyo ("Supreme Truth") is usually classified as a religious cult and, in fact, had official recognition as a religious group under Japanese law from 1989 to 1995.

states such as Iraq, that also sponsor terrorist organizations, appear to have access to, or the ability to manufacture, a range of chemical and biological weapons. World-wide, there have been several incidents of chemical or biological weapons being used by terrorist organizations in an actual attack. The United States Federal Bureau of Investigation characterizes weapons of mass destruction as "...perhaps the most serious potential threat facing the United States today". In 1997, the Federal Bureau of Investigation investigated over 100 threats or incidents involving nuclear, chemical or biological materials.[18] In fact, the United States claims that the list of states that sponsor terrorism produced annually by the Secretary of State corresponds almost exactly to the Central Intelligence Agency's list of states that have a chemical or biological weapons capability.[19] As for Canada, a package that may have contained a biological or chemical weapon was discovered by police in Edmonton.[20] A United States' resident with ties to white supremacist groups was arrested by authorities in December 1995 trying to smuggle 130 grams of Ricin from Canada into the United States.[21]

Basic chemical and biological weapons are relatively easy to produce and the "recipes" for a broad range of such weapons are readily available on the Internet and through the underground press. A terrorist with very basic technical knowledge could manufacture a chemical agent and build an effective device to detonate and disseminate the agent with relative ease. The manufacturing, detonation and dissemination of a biological device is more challenging and there is a higher risk of self-contamination for the terrorist.

Consensus among experts in the field is that the likelihood of a terrorist incident involving a nuclear, biological or chemical weapon is low in Canada. Notwithstanding the low risk, the consequences of a nuclear, biological and chemical incident in casualties and in psychological effect would be enormous. As a consequence, Canadian and other governments are taking measures to counter the threat and to combat an actual incident.[22]

"Cyber-Terrorism": In 1989, the Internet was not nearly as ubiquitous as it is today and the security threat it presents was not as widespread. Today, any nation that relies on computer systems is vulnerable to cyber- terrorism. In Canada, this includes our defence, telecommunications, energy, air traffic and banking systems; indeed most of the governmental and private systems we rely on daily. Marshall McLuhan wrote that "World War III would be a guerilla information war with no division between the civilian and military populations."
Louis J. Freeh, Director of the United States Federal Bureau of Investigation has characterized

---

[18] Louis J. Freeh, Statement before the United States Senate Judiciary Committee, Washington, D.C., September 3, 1998.

[19] Speech by Richard Clarke, National Coordinator for Security, Critical Infrastructure Protection and Counter-Terrorism to the Jane's Information Group, Washington, D.C., October 6, 1998.

[20] The package was destroyed before its contents could be analysed and the type of device confirmed.

[21] "Man Accused of Possessing Lethal Toxin Hangs Himself, AP Newswire, December 23, 1997.

[22] See Chapter III.

Canada as a "hacker haven" because of our sophisticated information technology system and our open society. According to evidence given to the Committee, a Sudbury man was recently charged with 27 counts of hacking into government and university computers in the United States and Canada.

No evidence of a major cyber- attack against Canadian critical infrastructures in Canada was given to the Committee. However, there has been a number of minor incidents in Canada and a number of incidents (or alleged incidents) elsewhere. These include incidents involving the Federal Bureau of Investigation and NASA websites in the United States, downloading top secret information from the computer systems at India's Bhabha Atomic Research Centre and shutting down a communications satellite operated by the Peoples' Republic of China. A few of the groups involved, including the group that claims to have shut down the Chinese satellite, are based in Canada, making use of our highly sophisticated and international information technology systems to mount actions abroad.

Cyber terrorism is extremely difficult to guard against. Cyber terrorists are often well educated, with the expertise and equipment to stay ahead of advances in protective security. Yet, the havoc wreaked by a major cyber-attack could be enormous. An illustration is to imagine that the power outages that affected Eastern Ontario and Quebec in January 1998 were brought about by a major cyber-attack, rather than by an ice storm. The Committee was advised by government witnesses of the steps being taken by the Government of Canada to protect against cyber- terrorism.[23]

Taking Credit: The established norm of behaviour used to be that terrorist groups would announce their threats and rush to take credit for their actions. In this way, their existence and their objectives would be as widely-known as possible.

A new trend is for terrorists not to take responsibility for their actions. The destruction, killing or maiming of targets is sufficient to the cause. Eschewing responsibility also avoids the prospect of retaliation, as occurred with the United States' bombing of Libya in 1986 in retaliation for a bombing attack on a German pub frequented by the United States soldiers. Not taking credit does not necessarily avoid retaliation, however. No group or individual took responsibility for the August, 1998 bombings of the United States Embassies in Nairobi and Kenya. Notwithstanding, the United States retaliated against the suspected perpetrators by bombing a terrorist training facility in Afghanistan and a chemical plant in The Sudan.

The trend to avoid responsibility makes it more difficult to track terrorist organizations, to trace responsibility for terrorist acts and to bring those responsible to justice.

Economic Espionage: With the end of the Cold War, competition among states became less military and more economic. Whereas states previously engaged in espionage primarily for military and foreign policy purposes, intelligence operations are now concentrating more on conducting, or guarding against, economic espionage. Economic espionage is rarely equated with terrorism.

---

[23] See Chapter II.

However, rogue states that sponsor terrorism may engage in economic espionage as an alternative to conventional terrorism. Furthermore, large, sophisticated terrorist organizations with the resources to do so may decide to engage in economic espionage as another terrorist tactic. An increasing number of states, including the United Kingdom, United States, Australia, South Africa and Russia have made public announcements about using their intelligence organizations both to conduct and protect against economic espionage. Some countries such as the United Kingdom have included protecting or advancing the state's "economic well-being" within the official mandates of their intelligence organizations. The French have expanded their criminal law on espionage to cover industrial and commercial espionage.

Canada's advanced industrial and technological society and our expertise in certain sectors, such as telecommunications, agriculture and fisheries, make us attractive to economic spies. Factors that make us vulnerable to economic espionage include the level of foreign ownership in our economy, the number of multinational corporations with operations here and the number of foreign students studying in Canada in the basic and applied sciences.

The true extent of economic espionage is impossible to gauge. Governments and private sector companies may not know that their secrets have been stolen until long after the event, if ever. Many companies do not report incidents of economic espionage out of embarrassment, or for fear of stock market or other negative consequences for the company.

Within our security intelligence establishment the Canadian Security Intelligence Service is, more than any other organization, charged with guarding against economic espionage. Under section 16 of *Canadian Security Intelligence Service Act,* the Canadian Security Intelligence Service also has the mandate to assist the government in the collection of information or intelligence "relating to the capabilities, intentions or activities" within Canada of a foreign state or group of foreign states, or persons other than Canadian citizens, permanent residents or special act corporations. The Canadian Security Intelligence Services mandate, however, applies to government: protecting the Canadian government against economic espionage and guarding against economic espionage against Canadian targets by foreign governments. The Canadian Security Intelligence Service' mandate does not extend to company to company espionage, unless it reaches the point of being "detrimental to the interests of Canada" under subsection 2(b) of the *Canadian Security Intelligence Service Act.*

Advances in Technology

> *"The same forces of technology that offer new economic and social opportunities also create new dangers. Terrorists'... methods are now more sophisticated."* United States President Bill Clinton

In addition to computer and information technology, there has been a host of other technological advances since the last Senate Special Committee on Terrorism and Public Safety reported. As with most such advances, they cut both ways: They may provide authorities with more efficient and effective methods of monitoring and interdiction, but probably also provide terrorists and other security threats additional means to pursue their own ends.

The panoply of technological advances with security or intelligence implications is too extensive to canvass in this Report. To both illustrate and focus attention on the threats posed, the Committee draws on four examples that were identified by witnesses as priorities: satellite imagery, encryption technology, cash debit cards and global telecommunications satellites.

Satellite Imagery or Space Borne Remote Sensing Technology involves the use of optical and radar satellites[24] to take images of the earth's surface. There are issues raised by this technology that have an impact on the security of Canada and of other states. Space borne remote sensing and the images it generates used to be the exclusive preserve of the military. Today, however, a number of countries offer satellite images to the public on a commercial basis.[25] These include current images and images from archives that have been declassified. This is referred to as "open source imaging". In some cases satellite images with a resolution of two metres are on the market for about $300 (USD). Furthermore, the resolution of satellite imagery is improving. Imagery from the EROS A satellite, scheduled for launch in late 1998, will generate panchromatic (black and white) images with a resolution of 1.5 metres, meaning that objects of one and one-half metres or larger will be readily identifiable. By a process known as "resampling", resolution can be further enhanced by the recipient or purchaser using computer technology. Resolution will inevitably continue to improve. Although the information is classified, experts in the field believe that the resolution of current United States' military satellite imagery is about 35cm. In the United States, Presidential Decision Directive 23 (March, 1994) authorizes the commercial availability of satellite images with resolution as good as 0.8 metres.

The potential for terrorist groups, economic spies and other security threats is obvious. Satellite imagery of high resolution and low cost could be used to "penetrate" sites that are otherwise inaccessible; or to evaluate security weaknesses at military, nuclear power or other sensitive facilities. The United States government exercises what is called "trigger control" over satellites it regulates. This means that, without express government approval, images of identified areas or facilities cannot be taken. No trigger controls currently apply to satellites under Canadian jurisdiction. In any event, there are serious questions as to whether trigger controls are effective in guarding against security threats. Even if trigger controls in one country are effective, identical satellite images are probably available from other countries that have no, or less restrictive, trigger controls. Furthermore, satellite images are not supposed to be sold to countries listed on the United Nations "blacklist". However, authorities acknowledge that, in practice, the use of intermediaries makes such a prohibition virtually unenforceable.

---

[24] Optical satellites are "passive". They receive energy transmitted or reflected from the earth in varying wavelengths and that data is used to identify different surfaces or covers of the earth's surface. Radar satellites use active sensors. They send out conventional radar waves and measure the return waves to identify different surfaces or covers. Optical satellites generally have better resolution than radar satellites.

[25] **Commentary Number 75**. "Exploiting the New High Resolution Satellite Imagery: Darwinian Imperatives?" Canadian Security Intelligence Service, (Ottawa), Summer, 1998.

Open access to images from space borne remote sensing already constitutes a potential threat. That threat will grow as resolution improves and as the availability of images expands.

Information Technology: Without doubt, the most significant technological advance since 1989 has been the growth of the Internet. The Internet provides the electronic tools for cyber- terrorism, money laundering and for more effective and secure communications among terrorist groups. Virtually every terrorist organization of note or its "front" organization has its own website. The Internet provides an unprecedented security threat because it is beyond effective regulation by any government and communications over the Internet can be made undecipherable.[26] The difficulties of effectively monitoring cyber- traffic presents a major challenge in monitoring the intentions and actions of terrorist groups and monitoring some of their transactions such as money laundering.[27]

Cash Debit Cards have recently been launched in Canada for market testing.[28] In essence, one may purchase a cash debit card with a pre-determined limit and draw down on that card for purchases until the limit is exhausted. The challenge for law enforcement agencies is clear: cash debit cards can facilitate money laundering by terrorist and other groups. The cards can be transferred from person-to-person and the transfers are effectively untraceable. The money can be accessed by the end user for nefarious purposes. Although current cards introduced in Canada have a relatively low limit ($1,000.00), witnesses before the Committee expressed concern that it is inevitable that the limits would rise to substantial sums.

Global Telecommunications Satellites will soon be available to provide digital cordless telephone connections from anywhere to anywhere in the globe. On the down-link from the satellite, the call can be received by another cordless telephone or can be connected into the Public Switched Telephone Network (PSTN). Iridium North America Inc. based in Arizona, has promised to launch the first world-wide wireless telecommunications system through a network of 66 satellites.

On one hand, the advantages of such a system are clear. People will be "connected" wherever they travel, even in remote areas of the world that have no terrestrial communications network and they will have one telephone number wherever they go. The challenges for law enforcement and security intelligence agencies are equally clear. It will become increasingly difficult to intercept or to identify the origins and destinations of telecommunications.

---

[26] The federal Department of Industry issued a public consultation paper "**A Cryptography Policy Framework for Electronic Commerce**" (February 1998). One alternative put forward in the paper is a key escrow system, whereby the key to decipher any electronic cypher code is held in escrow for access by law enforcement and other authorities via a search warrant. After a period of public consultation, Industry Canada decided not to proceed with a key escrow system, ("Canada's New Cryptography Policy", Industry Canada, October 1, 1998). A key escrow system has all but been rejected in the United States as well.

[27] See Chapter III.

[28] The first pilot project was conducted in Guelph, Ontario and has been completed. Another pilot project is scheduled to be launched in Sherbrooke, Quebec during the Spring of 1999.

Committee Observations and Recommendations

The direct threat from terrorism to Canada and Canadians has remained virtually unchanged over the past decade. Canada is still primarily a venue of opportunity to support, plan or mount attacks elsewhere and as a conduit to the United States. Terrorist groups are, however, present in Canada, some with substantial infrastructures and engaging in a range of criminal activities, albeit short of outright violence for the most part.

What has changed world-wide is the tactics available to terrorists. Those tactics have broadened and at least some terrorists have shown both a willingness and an ability to use new and potentially devastating weapons. Perhaps the most worrisome relate to advances in technology, particularly in information technology. On one hand, such advances can be used to improve the capability of security intelligence agencies to monitor and counter terrorist activities. On the other hand, technological advances enable terrorist groups to circumvent and otherwise frustrate the activities of security intelligence agencies and to engage in types of activities, such as cyber- terrorism, unforeseen even a decade ago. Furthermore, technology will continue to advance at an increasingly rapid pace. One can catch up today and find oneself behind tomorrow due to another technological advance.

No one reasonably expects our security intelligence community to reduce the terrorist threat to zero. Yet, because of technological advances, just keeping pace with terrorist organizations will require the investment of very considerable amounts of money by the federal government in countervailing technology. Due primarily to technological advances, governments cannot expect a "peace-dividend" in the security intelligence sector for the foreseeable future.

Careful consideration should also be given to rethinking current definitions of terrorism including the definition of "threats to the security of Canada" in subsection 2(c) of the *Canadian Security Intelligence Service Act*. Definitions that require violence or the threat of violence do not address modern tactics available to terrorists due to advances in technology and changes in tactics. The Committee suggests a definition that reflects the "gray-zone phenomenon" and incorporates threats to the stability of states.

CHAPTER II

RESPONSE TO RECOMMENDATIONS OF THE SENATE SPECIAL COMMITTEES ON TERRORISM AND PUBLIC SAFETY

The Senate Special Committees on Terrorism and Public Safety that reported respectively in 1987 and 1989 made a total of 37 specific recommendations.[29] It is not this Committee's intention to review the extent to which actions have been taken in response to each recommendation. Because of the major changes in the security environment over the past decade, such an exercise would not be particularly helpful. What this Committee did was group the recommendations on the basis of themes and analyse the responses, or the current situations, accordingly.

Overview

When the Senate Special Committees on Terrorism and Public Safety undertook their reviews, the federal government's security and intelligence sector was in the midst of a major transition. The Canadian Security Intelligence Service had just been set up as Canada's civilian security intelligence organization, the function having been transferred from the Royal Canadian Mounted Police as a consequence of the recommendations made by the McDonald Commission.[30] Allied security intelligence organizations expressed some bewilderment at the transfer of responsibilities from the Royal Canadian Mounted Police to the Canadian Security Intelligence Service and were concerned about how the Canadian Security Intelligence Service would work. The *Security Offences Act* had come into force in 1984, two effects of which were to clarify responsibilities and to highlight a number of jurisdictional issues that had to be addressed.[31] There was a complex of international conventions and treaties, some recently in place and others under negotiation, relating to terrorism. In addition, of course, Canada had been shocked by several recent terrorist incidents that challenged Canadians' perception of their country as a "peaceable kingdom", largely immune from the scourge of terrorism. The previous Special Committees' review of those incidents brought to light a number of problems that caused those Committees to question whether Canada was, in fact, adequately prepared to deal with the rising tide of terrorism.

The security and intelligence community that appeared before the Senate Special Committees on Terrorism and Public Safety over a decade ago was, perhaps understandably, one that was trying to find its way. Many departments and agencies were dealing with new or significantly changed mandates. Some of those departments or agencies appeared unable or unlikely to meet the

---

[29] 23 recommendations in the 1987 Report; 14 recommendations in the 1989 Report.

[30] The Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police.

[31] Particularly pursuant to s.s. 4(1), 4(2), 6(1) and 6(2) of the Act.

challenges from either a personnel or an organizational point-of-view. There also appeared to be a lack of central leadership or coordination. Officials who testified before the previous Senate Special Committees sometimes appeared defensive, even evasive.

This Committee remarked on a virtual sea of change in the security and intelligence community since 1989. The change encompasses a substantially higher degree of confidence, professionalism and evident competence among senior officials. The Committee also noticed a clearly stronger, better defined central leadership and coordination from the Privy Council Office as well as far more clarity in and understanding of individual organizational roles and jurisdictional responsibilities. This Committee wishes to commend officials and the government for the very considerable progress made in this regard.

International Arrangements

To be effective, the fight against terrorism must be through a united international front, based on international law as established through international agreements. Canada has exercised and continues to exercise a prominent role in the international community's development of a legal framework to counter terrorism and to bring terrorists to justice.

Table 2

Date	Convention
1963 Tokyo	Convention on Offences and Certain Other Acts Committed on Board Aircraft
1970 The Hague International Agreements Pertaining to Terrorism	Convention for the Suppression of the Unlawful Seizure of Aircraft
1971 Montreal	Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation
1988 Montreal	Protocol for the Suppression of Unlawful Acts of Violence at Airports Servicing International Civil Aviation
1991 Montreal	Convention on the Marking of Plastic Explosives for the Purpose of Detection

Date	Convention
1988 International Maritime Organization	Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation
1988 International Maritime Organization	Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms located on the Continental Shelf
1973 United Nations	Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents
1979 United Nations	Convention Against the Taking of Hostages
1979 United Nations	Convention on the Physical Protection of Nuclear Materials
1998 United Nations	Convention for the Suppression of Terrorist Bombing Offences

Table 2 lists the 11 international conventions signed by Canada relating to terrorism, of which Canada has ratified 10. The exception is the 1998 *United Nations Convention for the Suppression of Terrorist Bombing Offences*. In addition, negotiations on a *United Nations Convention on the Suppression of Acts of Nuclear Terrorism* are currently underway. Incidentally, these negotiations are being conducted under a Canadian chairman. Some of the major multilateral and bilateral initiatives taken since 1989 relating to counter-terrorism and involving Canada include:

- A G-8 conference on counter-terrorism research and development (December, 1997);
- Bilateral consultations on issues of specific interest to Canada were undertakenwith Cuba (1997), Israel (1997), India (1997,1998) and Spain (1998);
- Since 1988, the Canada-United States Bilateral Consultative Group ("BCG")[32]

[32] The Group consists of members of the security and intelligence communities of both countries and is co-chaired by Foreign Affairs and International Trade and the United States Department

has met annually to review counter-terrorism issues and the extent and nature of cooperation between the two countries;

- The 1995 P8 Ottawa Ministerial Declaration on Counter-Terrorism;
- The 1996 Sharm el-Sheikh Summit;
- The 1996 Summit Eight Ministerial Meeting in Paris; and
- There has been extensive security and intelligence cooperation for decades among Canada, the United States, Great Britain, Australia and New Zealand. This cooperation has continued to expand over the last ten years due in part to the rapid changes in the technology, weapons and tactics potentially available to terrorists.

Committee Observations and Recommendations

For a nation of Canada's size, effecting international agreements and relationships are absolutely essential to counter terrorism. The Committee is pleased with Canada's continuing commitment in this regard and the substantial progress that continues to be made.

The previous Senate Special Committees on Terrorism and Public Safety noted that international negotiations concerning terrorism often became tangled in a debate around the definition of terrorism and philosophical or ideological debates over the root causes of terrorism. These debates too often deflected negotiations from their course and delayed progress. This Committee was pleased to note that those debates have been largely surmounted. The *United Nations Declaration on Measures to Eliminate International Terrorism (1994)* saw a profound shift from a debate over definitions and root causes towards a concerted effort to deal with terrorism. Most countries now acknowledge terrorism as a crime.

It has long been recognized that international agreements and international law to a significant degree are as effective as the very strongest nation allows them to be. For many years that nation has been the United States, counterbalanced somewhat by the Soviet Union until it collapsed. For example, the United States' bombings of alleged terrorist targets in Afghanistan and Sudan, which it justified based on Article 51 of the United Nations Charter, may also be in conflict with the *International Convention for the Suppression of Terrorist Bombings.* The Convention has been endorsed by the G-8 and 20 other nations and was signed by Canada on January 12, 1998, but has yet to be ratified. The United States' action is taken by some commentators as evidence that the United States will be the *de facto* standard for compliance with international law relating to

---

of State. Members include representatives from the Canadian Security Intelligence Service, the Central Intelligence Agency, the Royal Canadian Mounted Police, the Federal Bureau of Investigation, the Solicitor General of Canada and Citizenship and Immigration Canada.

terrorism .[33]

Canada, as the United States' main trading partner and next door neighbour, not only will be affected by the United States' support for international agreements on terrorism, but also because of the importance of our two countries' cooperation and support for each other in the fight against terrorism, Canada is uniquely positioned to influence United States' policy and actions in this regard. The Committee recommends that the Government of Canada continue to use all legitimate means to do so.

The National Counter-Terrorism Plan (NCTP)

Probably the most serious thematic concern raised by the previous Senate Special Committees on Terrorism and Public Safety related to "Who does what?" What organizations and people are responsible and what are they responsible for during an actual terrorist incident? Who is really[34] responsible and what are they really responsible for? In this regard, the previous Senate Special Committees on Terrorism and Public Safety noted a lack of clarity or consensus on roles and responsibilities within the federal government and between the federal government on one hand and the provincial and municipal authorities on the other. In the previous Senate Special Committees' judgement, this situation created an environment conducive to turf battles that seriously detracted from our ability to respond to a particular incident in the most effective way. Perhaps the best illustration of the previous Committees' concerns was the Bahamian High Commission incident where a dispute broke out between the Royal Canadian Mounted Police and the Ottawa Police Force as to who was in charge while the incident was underway.

Progress made since 1989 has been remarkable. Disagreements between federal authorities on one

---

[33] In particular, articles 17 and 18. Canada's Foreign Affairs Minister, Lloyd Axworthy, supported the United States' action based on "credible evidence" from Secretary of State Madeleine Albright that United States' assets or interests were, in fact, threatened. Foreign Affairs and International Trade officials also advise that the bombings were exempted from the Convention pursuant to Article 19(2). Article 19(2) exempts "activities undertaken by military forces of a State in the exercise of their official duties inasmuch as they are governed by other rules of international law". Foreign Affairs and International Trade officials also point out that states continue to sign the Convention in a prompt manner, even those who opposed the bombings and those who opposed inclusion of Article 19(2) in the Convention.

[34] The previous Senate Special Committees found, to their dismay, that organizational responsibilities as set out in various written documents were often not followed in practice. For example, notwithstanding the Solicitor General's principal role for co-ordinating the federal government's response to a terrorist incident in Canada, for each major incident studied by the Special Committees, actual coordination had been conducted by the Privy Council Office under the direction of the Deputy Prime Minister. The Special Committees' view was that the manuals, in their description of procedures and responsibilities, should conform to practice, or vice versa. Otherwise the manuals play no useful role and only confuse responsibility and accountability.

hand and provincial and municipal police forces on the other hand as to who is in charge during a terrorist incident appear to have been resolved. Furthermore, municipal and provincial police forces who appeared before the Committee or were interviewed by Committee staff expressed complete satisfaction with the level of cooperation and assistance from federal authorities, in particular from the Canadian Security Intelligence Service and the Royal Canadian Mounted Police.

In response to the 1987 Report of the first Senate Special Committee on Terrorism and Public Safety, the government developed the first National Counter-Terrorism Plan ("NCTP"). In 1995, the Ministry of the Solicitor General decided that revisions to the Plan were called for in order to accommodate changes in the threat environment, such as the shift of responsibility for armed response to a serious terrorist from the Royal Canadian Mounted Police to the Department of National Defence.[35] That process resulted in an "Interim" National Counter-Terrorism Plan that was reviewed by this Committee.

The National Counter-Terrorism Plan is, in effect, the "manual" for responding to a terrorist incident, for both incident management and public communications purposes. As such, it is the critical reference for "Who does what?" during a terrorist incident. The National Counter-Terrorism Plan represents a positive advance. It clearly articulates what was not previously articulated and, by being articulated, reduces the potential for differing assumptions, misunderstandings or conflict.

The "Interim" National Counter-Terrorism Plan has been devised in consultation with provincial authorities and through them with the major municipal police forces. The consultation process has helped develop a Plan that is both workable in practice and one that is more likely to be understood and accepted by all levels of government.

As has been the case since 1985, under the Interim National Counter-Terrorism Plan the federal Solicitor General is the lead Minister for terrorist incidents occurring within Canada. The Minister of Foreign Affairs is the lead Minister for terrorist events outside of Canada involving Canadians or Canadian interests.

Committee Observations and Recommendations

The National Counter-Terrorism Plan is another illustration of the progress made on the counter-terrorism front within the Government of Canada. The Committee's detailed comments on the Interim National Counter-Terrorism Plan have been conveyed privately to the Solicitor General. The Committee acknowledges that the provinces have been consulted during the revisions to the National Counter-Terrorism Plan and the provinces have endorsed it.[36] Notwithstanding, the

---

[35] This shift had been recommended by the first Senate Special Committee on Terrorism and Public Safety.

[36] Two drafts of the National Counter-Terrorism Plan were sent to the provinces for comment. Representatives of the Ontario government complained that Ontario was given insufficient time to give fully-considered responses to the drafts. Ontario's "final" response is still outstanding as this Report was

Committee believes it imperative for each province actually to sign the National Counter-Terrorism Plan. This would confirm it as a truly "national" counter-terrorism plan, rather than a federal plan prepared in consultation with the provinces. The federal Plan should also constitute the action plan for each province's response to a terrorist incident. In those cases where provincial counter-terrorism plans exist, it should be clear that the federal Plan prevails in the event of any conflict or inconsistency between the federal and provincial plans.

The Committee is aware that two provinces have developed or are developing their own counter-terrorism plans.[37] Federal government witnesses assured the Committee that such plans are entirely consistent with the National Counter-Terrorism Plan and had been devised to specify provincial and municipal roles within the National Counter-Terrorism Plan. Committee staff were briefed on Ontario's Counter-Terrorism Plan and found a few inconsistencies with the National Counter-Terrorism Plan that are troubling. One inconsistency is that Ontario's Plan defines "terrorist activity" as "extraordinary violence or threats of such violence"[38], compared to acts or threats of "serious violence" under the *Canadian Security Intelligence Service Act,* whose definition is the foundation for the National Counter-Terrorism Plan. Ontario's Plan also specifies as follows:

> *"The original responding police service shall exercise "lead responsibility" unless or until that "lead" is transferred by mutual agreement of the police services who have responded. In the event of a disagreement, the original responding police service* ***shall immediately refer the issue to the Solicitor General for the Province of Ontario for a decision on how the Memorandum of Understanding is to be applied."*** [39] *(Emphasis added)*

When both the Royal Canadian Mounted Police and the Ontario Provincial Police or a municipal police force respond to a terrorist incident, this formulation would appear to conflict with the Royal Canadian Mounted Police's "primary responsibility" under section 6 of the *Security Offences Act.* Ontario and federal officials assured Committee staff, however, that in such instances, the provincial Solicitor General would be obligated to consult with the Solicitor General of Canada under the federal-provincial Memorandum of Understanding.

Of more concern to the Committee is the lengths to which the Ontario Plan goes to distinguish between "primary" and "exclusive" responsibility with respect to the Royal Canadian Mounted Police's authority under the *Security Offences Act.*[40] Ontario's position is that the Royal Canadian Mounted Police's primary responsibility relates to investigation of an offence and laying charges relating thereto under section 2 of the *Security Offences Act* and not necessarily to the response to

---

being finalized.

[37] Ontario and Manitoba. The development of Manitoba's plan was motivated by Winnipeg being selected as the venue for the Pan American Games.

[38] Emergency Measures Ontario, "Provincial Counter-Terrorism Plan", July 1998, subsection 2.2.

[39] Ibid., subsection 3.9.3.

[40] Ibid., subsection 3.6.

and management of a terrorist (or other security offence) incident.

The Ontario government and the Ontario Provincial Police also expressed concerns that the National Counter-Terrorism Plan needs more work to integrate the consequence management of an incident with the strategic and tactical responses. For example, the strategic response should include an assessment of the likelihood of retaliation by the terrorist group in the planning for the tactical response. In addition, Ontario feels that more clarity is required in procedures such as those to request military support.

Several witnesses emphasized the importance of the National Counter-Terrorism Plan being able to address effectively, not simply the current terrorist threats and tactics, but also the new ones as they emerge. The Committee agrees. For example, the new emerging threat of cyber-terrorism is of a fundamentally different nature from conventional terrorist threats and requires that the National Counter-Terrorism Plan be not only aware of emerging technologies, but indeed be on the leading edge in terms of capability.

In the Committee's view, another gap that exists in the National Counter-Terrorism Plan pertains to the media. The previous Senate Special Committees on Terrorism and Public Safety identified terrorist incidents where, in the previous Committees' view, members of the media had acted irresponsibly and by doing so had endangered life. Media coverage has been characterized as the oxygen on which terrorists depend and is crucial for a terrorist in order to convey the "terror"of an incident. The Committee was pleased to hear that the Royal Canadian Mounted Police and Ministry of the Solicitor General have developed a number of strategies to deal more effectively with the media during an incident, while respecting the media's role and constitutional freedoms. In addition, since the last Senate Special Committee on Terrorism and Public Safety reported, a public communications sub-group has been set up under the Interdepartmental Policy Advisory Group (see Chapter IV).

The previous Senate Special Committees on Terrorism and Public Safety were advised that the government hoped to work with the media to develop mutually-accepted guidelines for media conduct during a terrorist incident. No such agreement has been reached; no guidelines exist. While recognizing the difficult issues relating to the development and enforcement of such guidelines, the Committee urges the media and the government not to abandon the effort. In any event, the absence of guidelines does not absolve the media from a duty to act reasonably and responsibly during a terrorist incident.

The Committee has been advised that the National Counter-Terrorism Plan will not be treated as a static document but will be regularly reviewed and updated as required. The Committee strongly supports this commitment. The Committee also strongly supports the commitment made by government witnesses to periodic testing of the National Counter-Terrorism Plan through joint training and exercises.

The previous Senate Special Committees on Terrorism and Public Safety noted a lack of acceptance

or recognition of the Solicitor General's role as the lead Minister to counter terrorism in Canada. This was, in the Committees' view, exacerbated by the junior status of the Ministry of the Solicitor General and the need for more resources to give life to the Ministry's counter-terrorism mandate. The Committee has concluded that the Ministry of the Solicitor General's role appears to be better recognized and accepted across the Government of Canada.

While there is clearly enhanced recognition of the Solicitor General's overall responsibility for counter-terrorism contingency planning, for co-ordinating the response to a terrorist incident and for advising the Prime Minister and Cabinet in this regard, it is generally recognized – and indeed, this is recognized in the National Counter-Terrorism Plan – that in the event of a major terrorist incident the Prime Minister or Deputy Prime Minister may assume a lead role, supported by the Privy Council Office. Ongoing operational coordination is provided by the Interdepartmental Policy Advisory Group working in the Royal Canadian Mounted Police National Operations Centre. The Committee agrees. In our system of ministerial responsibility, this is entirely logical and appropriate.

Government witnesses before the Committee emphasized the importance of informal, personal relationships within the security and intelligence sector for purposes of day-to-day coordination. Such relationships are made more difficult where there are high turn-overs in senior personnel.

Illegal Migration

Each year there are about 110 million border crossings into Canada from the United States, about half of which involve returning Canadian citizens or permanent residents. Canada's immigration programs also generate up to 225,000 immigrants annually. In 1996, 125,000 applications for permanent residence in Canada were processed abroad, of which 77% were approved. Over 700,000 visitor visa applications are processed annually, of which about 90% are approved; and in 1998 (to September 30) the Canadian Refugee Determination Division received 17,020 applications for refugee status.[41]

The first Senate Special Committee on Terrorism and Public Safety reviewed Canada's immigration policies and procedures at length and concluded that they had been devised, or at least the fundamental principles and procedures set, before international terrorism became a major threat or concern to policy makers. As a consequence, the first Special Committee on Terrorism and Public Safety concluded that our immigration policies and procedures were ill-suited to the threat environment.

A review of developments with respect to immigration since 1989 is a good news/bad news scenario that can be summarized as follows: On the good news side, the Canadian Security Intelligence Service has developed "profiles" that enhance our ability to identify people applying to enter Canada who constitute security threats. Furthermore, the "silo" mentality noted by the

[41] Figures from Citizenship and Immigration Canada.

previous Senate Special Committees on Terrorism and Public Safety, wherein Immigration was isolated from the larger security and intelligence community, has broken down. Government and independent witnesses spoke about increased cooperation between Citizenship and Immigration Canada on one hand, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police on the other hand and a more effective integration of Citizenship and Immigration Canada into the security and intelligence community.

On the negative side, resource constraints may be adversely affecting our ability to weed out security threats. Witnesses before the Committee referred to a need for more technology to access data. Many consular offices have been closed or down-sized, resulting in a centralization of processing in major consular centres that are often geographically distant from the source of the people they are processing. They thus risk being out-of-touch with developments in those countries that, in turn, may raise security implications.

The first level of defence against illegal migration at Canadian ports of entry is the Primary Inspection Line ("PIL"). The PIL is staffed by Customs Officers who refer any suspicious entrants to Immigration officers. Some PIL officers complained to Committee staff about poor pay, lack of technical resources and pressure to process people quickly.

Another concern raised with the Committee is Canada's reliance on other countries' police or security intelligence agencies for vetting our immigration applicants. Some witnesses before the Committee and submissions to it suggest that Canada's requirements are not given priority.[42]

Although there have been instances of terrorists and other security threats gaining access to Canada as landed immigrants, of particular concern to the previous Senate Special Committees on Terrorism and Public Safety was Canada's refugee determination policies and procedures. It is a cornerstone of the *Immigration Act* that persons applying to live in Canada submit their applications outside Canada and obtain approval before entry.[43] Accordingly, persons applying for landed immigrant status, work or student visas must present at a Canadian consular office abroad and go through a process that includes security checks before they may be admitted to Canada. The majority of refugee claimants, on the other hand, make their claim upon arrival in Canada and remain in Canada while their claim is being processed. Security and criminal records checks cannot, therefore, be conducted in advance of their arrival in Canada.

The situation has not improved significantly since the previous Senate Special Committees on Terrorism and Public Safety reported. Illegal migration into Canada, primarily through our refugee determination system, persists as a concern from two perspectives. First, it is a means by which

---

[42] See Chapter III.

[43] **Immigration Policy - 5 (IP-5),** Citizenship and Immigration Canada, November, 1997, para. 1.2. This applies with two exceptions: the ability to claim refugee status after landing in Canada; and "in-land" applications for status for humanitarian or compassionate grounds under subsection 114(2) of the Immigration Act, by those who have no status in Canada or whose status (for example as visitors or students) has expired.

terrorists may circumvent our vetting process abroad and enter Canada in search of a temporary or permanent haven. Once here, they may conduct fundraising or other activities in Canada or, in a very few cases, to organize acts of violence in Canada or against other countries. Second, large volumes of illegal migrants provide the stream in which a few terrorists could ultimately gain entry to the United States by circumventing Canadian and United States' border controls.

During the first nine months of 1998, nearly 75% of the refugee claimants arriving at Canadian airports were improperly documented. During the same period, 65% of all improperly documented arrivals at airports presented no documents at all.[44] Although they are finger-printed, witnesses expressed concern that the quality of prints is poor because of inadequate training and equipment and, in any event, fingerprints are warehoused unless a problem with a particular claimant arises. The vast majority of people who arrive in Canada and claim refugee status are not detained, but are allowed to circulate freely in Canadian society pending a decision on their status. The *Immigration Act* authorizes immigration officers to impose terms and conditions on refugee claimants, but they usually extend no further than providing an address in Canada and an obligation to report at a specified time and location. According to the Report of the Immigration Legislative Review:

> *"There is no effective system in place to verify compliance with these terms and conditions. Thousands of persons awaiting inquiry or removal, or who are undergoing the refugee determination process are physically in Canada, and thousands of others have voluntarily left the country, but the department is not aware of their whereabouts."* [45]

At **Table 3** are the numbers of refugee claims abandoned or withdrawn over the past 10 years. Since Canada has no exit controls, it is impossible to calculate how many of these claims represent people who remain in Canada illegally, how many have slipped into the United States, how many have returned to their country of origin, or how many have gone elsewhere. As of October 23, 1998 there were 6,119 warrants for removal issued against persons deemed to have abandoned or withdrawn their refugee claims. Of these, 640 warrants have been executed and the persons removed from Canada, 240 warrants have been cancelled and there has been no action on the remaining 5,272 warrants.[46]

---

[44] Figures from Citizenship and Immigration Canada.

[45] **Not Just Numbers: A Canadian Framework for Future Immigration**, Minister of Public Works and Government Services Canada, (Ottawa, 1997), p. 103.

[46] Figures from Refugee Branch, Citizenship and Immigration Canada.

Table 3

Year	Abandoned	Withdrawn	Total
1989	44	82	126
1990	193	170	363
1991	664	695	1359
1992	812	937	1749
1993	2303	2329	4632
1994	2032	1458	3490
1995	2142	1144	3266
1996	3377	1764	5141
1997	3363	2300	5663
1998 (to September)	3064	1549	4613

Source: Citizenship and Immigration Canada.

In addition, there is a lengthy backlog for reviewing refugee claims that are not withdrawn or abandoned. When Citizenship and Immigration Canada officials appeared before the Committee, there was a backlog of 27,000 refugee claimants in the system. As of September 30, 1998, there were 23,924 claims pending before the Immigration and Refugee Board. The average time for a refugee claim to be processed from the initial claim to the final determination is 12 months.

A significant number of refugee claimants are brought into Canada by organized smuggling rings. Canadian and United State' authorities briefed Committee staff on how the rings operate and a summary description is set out in **Table 4**. The evidence before the Committee indicated that these rings generate substantial profit from smuggling and in some cases involve organized crime. There is concern that such rings could also be used to smuggle terrorists. The Committee was pleased to learn of the extensive efforts being made to halt such smuggling, including joint efforts of Canadian and United States' authorities, police organizations (e.g. the New York State Police, the Royal Canadian Mounted Police and the Ontario Provincial Police) and the respective immigration and customs authorities that are working together to address this serious problem.

Table 4

A Case Study in Smuggling Aliens

Persons wishing to enter Canada who have failed to obtain entry visas, board commercial flights overseas. When they board, they have their personal identification and other documents in hand for inspection by government and airline personnel in the country of embarkation.

At some time during the flight they dispose of their documentation or turn over all their documentation to the smuggler who has accompanied them on the plane. [The smuggler is usually a well-dressed "businessman" sitting in business class or first-class who often passes unchallenged through Canadian Customs and Immigration.]

On arrival at a Canadian port of entry they claim refugee status and often, as is their right, refuse to divulge any personal information. Unless they fit a security profile they are released pending a refugee hearing. It is rarely possible to perform other than a cursory security or criminal records check at this point.

Upon leaving the airport they are picked up by the smuggler and either go underground in Canada or are transported across the border into the United States. A favourite conduit to the United States, known as "Smugglers' Alley" to the authorities, is the Akwesasne Reserve near Cornwall, Ontario. Once in New York State, they are released.

Committee Observations and Recommendations

The Committee underscores the value of immigration to Canada, both past, present and future and the important role immigrants and their descendants play in Canada's society and economy. The Committee also acknowledges that, contrary to public perception, crimes committed by visitors, refugee claimants, refugees and immigrants are proportionately less than crimes committed by the general Canadian population.[47] *The Committee's recommendations or observations are intended to enhance proper immigration and refugee policies.*

The McDonald Commission, the House of Commons Special Committee on the Review of the *Canadian Security Intelligence Service Act* and the *Security Offences Act* and the Special Committee on Terrorism and Public Safety (1987) each noted that the definition of a threat to the security of Canada in section 2 of the *Canadian Security Intelligence Service Act* is materially different from the "security exclusion" provisions of the *Immigration Act*.[48] The Committee urges the government

---

[47] **Not Just Numbers**, op cit. p.p. 102-103.

[48] Part III of the Immigration Act lists in section 19(a) number of grounds that render persons inadmissible to Canada. Subsections 19(1)(e) through 19(1)(g) list the security exclusions including "persons who (sic) there are reasonable grounds to believe...will engage in terrorism...or are members of an organization that (sic) there are reasonable grounds to believe will...engage in terrorism...or

to bring those definitions into line as part of the current review of the *Immigration Act*.

Otherwise, deficiencies in Canada's immigration policies and procedures appear to be primarily a factor of resources, rather than gaps or inadequacies in the legal framework. In the Committee's view, it is imperative that Citizenship and Immigration Canada has the technical, personnel and other resources necessary to protect the security of Canada and Canadians. The Committee is concerned about the very substantial year-over-year increases in abandoned refugee claims, the likely number of those who have gone underground in Canada or the United States and our apparent inability to locate and execute removal orders against those who remain in Canada illegally. There must be a more effective tracing and enforcement system to keep track of refugee claimants and other non-status persons in Canada.

The persistent problems with our refugee determination system need to be addressed. There are several indications that serious problems persist: the number of claimants who "disappear" and are untraceable by Citizenship and Immigration Canada, the perception that our system is leaky and our enforcement system overwhelmed, the perception that it is in claimants' interests **not** to comply with our immigration rules, terms and conditions[49] and the ability of smugglers to subvert the system to their own commercial ends. The Committee recognizes however, that it is difficult to clamp down on illegal migration without harming the many *bona fide* refugees who seek a haven in Canada.

The Committee suggests, however, that Canada owes an obligation to its neighbours not to expose them to undue security risks through a porous refugee determination system. It may be that eventually Canada and the United States will move towards an integrated and common approach to immigration into North America, as appears to be happening incrementally among the nations of the European Union. This would, however, have far-reaching consequences, beyond issues of immigration and security and is beyond the scope of this Committee's mandate.

In the meantime, it is critical that Canada address the growing problem of the smuggling of aliens. Witnesses before the Committee confirm that the same gangs that smuggle aliens are also usually involved in the smuggling of firearms, tobacco, beverage alcohol, drugs and credit cards.

In fact, the smuggling infrastructure was originally created to smuggle tobacco. When tobacco smuggling became less lucrative due to the federal and provincial tax roll-backs in February, 1994, the smugglers simply shifted to other commodities. Groups engaged in smuggling are also often involved in other criminal activities such as money laundering. Accordingly, the smuggling of aliens is one part of a much wider public policy issue. It must be addressed in a horizontal way using the resources of all levels of government on both sides of the border. The Committee strongly recommends that Canada continue and expand the efforts now underway to take concerted action against this smuggling, using the combined resources of the Royal Canadian Mounted Police, the

---

persons who (sic) there are reasonable grounds to believe ...have engaged in terrorism." Nowhere is "terrorism" defined. This wording is much more restrictive than subsection 2(d) of the Canadian Security Intelligence Service Act.

[49] **Not Just Numbers**, op cit, section 8.2 "A Lack of Compliance", p. 102.

local and provincial police forces, Immigration and Customs authorities and, in particular, including the United States counterparts of these authorities.

Fundraising

A variety of groups with terrorist affiliations conduct fundraising activities in Canada. Intimidation and various other forms of coercion within the various emigré communities are often used as fundraising tactics.

It is very difficult to police terrorist fundraising. Intimidation and other illegal tactics are rarely reported. Terrorist groups often use benevolent or philanthropic organizations as fronts for fundraising purposes. These benevolent or philanthropic groups may even be registered as charities or charitable foundations by Revenue Canada under the *Income Tax Act*. Such status enhances the credibility of such groups and, ironically, creates the situation where Canadian taxpayers subsidize their activities. People from whom funds are solicited usually have no idea that they will be put to other than legal purposes. Drawing a clear connection between funds raised in Canada and a terrorist action elsewhere is often impossible. Fundraising front groups usually take care to commit no crime in Canada. Under existing law, the only viable charge is conspiracy if a direct connection can be established between the funds raised in Canada by such groups and illegal activity elsewhere.

The United States has tried to get at terrorist fundraising through the *Antiterrorism and Effective Death Penalty Act, 1996 (AEDPA)*. Section 302 of that Act authorizes the Secretary of State to designate as Foreign Terrorist Organizations ("FTO's") groups that meet specified criteria. The *Antiterrorism and Effective Death Penalty Act* makes it an offence to knowingly provide, or conspire to provide, material support or resources to an FTO. In addition, once designated as an FTO, any terrorist group's funds held by a financial institution subject to United States law must be blocked by that institution. The financial institution is required by the *Antiterrorism and Effective Death Penalty Act* to report the existence of such funds to the Secretary of State and follow the Secretary of State's directions as to their disposition.

It is too early to judge the effectiveness of the *Antiterrorism and Effective Death Penalty Act* in this regard. The Federal Bureau of Investigation allows investigations to establish relationships between legal front groups and terrorist groups and to trace funds which are complex, time-consuming and require substantial personnel and other resources.[50]

[50] Louis J. Freeh, Statement to the United States Senate Judiciary Committee, Washington, D.C. September 3, 1998.

Committee Observations and Recommendations

Addressing the problem of fundraising by groups with terrorist affiliations presents a public policy conundrum to which the Committee has no novel solution.

The problem of such groups having charitable registration can, however, be more effectively addressed. The Committee recommends that consideration be given to amending the *Income Tax Act* to allow Revenue Canada to deny charitable registration to any group on the basis of a certificate from the Canadian Security Intelligence Service. The certificate would be issued by the Canadian Security Intelligence Service if the group constitutes a threat to the security of Canada, as defined in the *Canadian Security Intelligence Service Act*. Care would have to be taken in drafting the provisions to ensure that the Canadian Security Intelligence Service's decision is made according to a defined procedure, adequately reviewable by the Security Intelligence Review Committee and the Courts on application by the group and in accordance with the *Charter of Rights and Freedoms*. Care should also be taken to avoid a situation where the certificate becomes a bargaining chip in obtaining cooperation from such groups.

Airport Security

Major changes have occurred that impact on airport security since the last Senate Special Committee on Terrorism and Public Safety reported in 1989.

In the first place, the majority of Canada's airports have now been privatized and are now owned and operated by local airport authorities. In the second place, responsibility for protective and security operations at airports has been transferred from the Royal Canadian Mounted Police to local police forces. In Vancouver, the Royal Canadian Mounted Police is the police force of local jurisdiction and has been contracted by the Vancouver Airport Authority to provide policing and security services.

When an airport is privatized[51] federal legislation requires the airport authority to assume responsibility for airport security, including the provision of policing and security functions, but the Minister of Transport regulates areas in which airport security personnel must be trained.

As before, personnel who screen passengers in the pre-boarding phase are contracted by the air carriers and trained in accordance with Ministry of Transport standards. Local police forces also enter into a contract with the airport authority to provide airport protection and security. In addition, a Memorandum of Understanding ("MOU") is entered into by the Royal Canadian Mounted Police and the local police force that specifies respective roles and responsibilities, in particular with respect to incidents falling under the *Security Offences Act*. In essence, the Memorandum of Understanding prescribes that matters that fall within the jurisdiction of the *Security Offences Act*

[51] In this context "privatization" means the transfer of operational and financial responsibility for an airport from the federal government to a duly-constituted airport authority.

are the responsibility of the Royal Canadian Mounted Police. Matters of a criminal nature that are not under the *Security Offences Act* fall under the jurisdiction of the local police force.

Although both the Royal Canadian Mounted Police and the local police force would likely be involved in managing either type of incident, in the case of a terrorist incident, the Royal Canadian Mounted Police would assume lead responsibility and the National Counter-Terrorism Plan would come into play. The Royal Canadian Mounted Police has authorized the establishment of a National Security Investigations Sections at 10 designated international airports. All but two are now operative.

Committee Observations and Recommendations

The previous Senate Special Committees on Terrorism and Public Safety identified "turf battles" between the Royal Canadian Mounted Police and the local police forces as a major issue affecting airport security and affecting Canada's ability to respond to a terrorist incident at an airport. Having local police forces responsible for airport protection and security is entirely consistent with the previous Committees' recommendations and is endorsed by this Committee. The respective roles and responsibilities of the Royal Canadian Mounted Police and local police forces have been clarified and appear to be accepted by all parties. This constitutes a major and positive step.

The Committee hopes that the Royal Canadian Mounted Police retains some visibility at international airports in Canada. The Royal Canadian Mounted Police uniform is a well-known and respected identifier for the travelling public and perhaps a deterrent to terrorists and criminal elements.

A fundamental question persists: Does the demarcation in responsibility between the Royal Canadian Mounted Police and the local police force make practical sense? Is that demarcation likely to cause confusion during an incident that could interfere with an effective response and interfere with effective incident management?

This issue was crystallized for the Committee in the response by officials to a hypothetical "scenario" involving the Royal Canadian Mounted Police and Peel Regional Police at Pearson International Airport.

> *"...Peel Regional is the lead agency in the event that terrorists hijack an aircraft and the Royal Canadian Mounted Police is the lead agency in the event that "politically motiviated" (sic) terrorists hijack the same aircraft..."*

First of all, "terrorism" is usually taken to be covered under subsection 2(c) of the definition of threats to the security of Canada under the *Canadian Security Intelligence Service Act.* Subsection 2(d) refers to "activities...directed towards or in support of serious violence...for the purpose of achieving a political objective..." By current definition, therefore, terrorism is politically motivated; there is no other kind. More important, however, is how things would work in practice. How does

one know if a hijacking is criminal (and thus is the responsibility of the local police force) or terrorist (and thus the responsibility of the Royal Canadian Mounted Police)? Will responsibility shift and will the shift be performed smoothly?

In the absence of examples of the system breaking down, the Committee is prepared to accept that it will work. The key, as far as the Committee is concerned, is joint-training and exercises conducted regularly between the Royal Canadian Mounted Police and the local police forces to make sure the system works flawlessly during an actual incident.

There has been no terrorist attack involving a Canadian airport or a Canadian aircraft since the last Senate Special Committee on Terrorism and Public Safety reported. Notwithstanding, in March, 1998 a mentally unbalanced person managed to gain access to the cockpit of a plane sitting at a passenger bridge at Pearson International Airport. When challenged by security screening guards, the individual sprinted to the nearest open passenger bridge where a plane was ready for boarding. The incident was handled quickly without injury to anyone else and without damage to property.

The incident does raise concern about the effectiveness of that airport's security, and should not have happened. It calls into question the effectiveness of baggage and personal checks by private security screening guards if the guards are not able to stop an obvious threat when it happens.

The Committee recognizes that increased security often slows passenger flows and increases inconvenience. The Committee reluctantly accepts representations by Transport officials that it would not be cost-effective to institute further security procedures or equipment at airports such as doors that automatically close in response to an alarm.

CHAPTER III

EMERGING ISSUES

Overview

Since the reviews conducted by the previous Senate Special Committees on Terrorism and Public Safety, several new issues of relevance to security and intelligence have arisen. These issues include the protection of Canada's critical infrastructures from terrorist penetration or sabotage, Canada's approach to encryption policy, the threat assessment capability of the government of Canada and the consumption of intelligence generated by the security intelligence community.

Protection of Critical Infrastructures

Critical infrastructures are both physical and cyber-based systems essential to the day-to-day operations of the economy and government. Critical infrastructures include, but are certainly not limited to, telecommunications, energy, banking and finance, transportation, water, sewage and emergency systems. Historically, critical infrastructures were physically segregated. Because of advances in technology, however, critical infrastructures have progressively converged and have become linked, sometimes interdependent. Advances in technology have also resulted in a high and growing level of automation in the operation of critical infrastructures. The growth of and our increased reliance on critical infrastructures, combined with their complexity, have made them potential targets for physical or cyber-attacks.

Canada is one of the most advanced nations of the world in terms of power generation and transmission, telecommunications and information technology. Canada has become an information-intensive society and economy. These advanced technologies and infrastructures have greatly assisted Canada in bridging our vast geography and enhancing our global interconnections, but have also increased our vulnerability to potential terrorist disruption.

Not surprisingly, the rapid advances in interconnections and information technology create a huge challenge in protecting the systems from intrusions and perhaps even sabotage. This is particularly true where various generations of systems are connected, making the older and less sophisticated a potential entry point through which to attack the entire system.

Witnesses before the Committee, from various government agencies, used the example of the recent ice storm to illustrate their concern with the devastating impact a serious disruption in our critical infrastructures could have on Canadian lives and indeed on the security of the country. The

Committee heard repeated evidence from witnesses, including the Solicitor General,[52] of efforts under way to protect our critical infrastructures. The Committee was informed that this effort is being coordinated at a senior level in the Privy Council Office and that international efforts are also underway to address these very serious risks.

With the explosion in new technologies, government departments and agencies responsible for the security of Canada's critical infrastructures have a major challenge to address. The results of vulnerability tests performed in certain departments to replicate a cyber-attack have not been comforting. The Committee was assured that federal departments and agencies are well aware of the challenges and that they have much to do to meet them; but they are confident that they can do it. Canada's close cooperation and mutual interest with the United States in this regard should be very helpful.

The United States has taken concerted measures to address the vulnerability of their government and private sector critical infrastructures beginning with Presidential Directive 39 in 1995. That Directive created a small interdepartmental task force (the Critical Infrastructure Working Group, or "CIWG"). In its 1996 report, the Critical Infrastructure Working Group recommended development of a national strategy to protect critical infrastructures and an interim group to coordinate the federal government's existing assets should an infrastructure attack occur (the Infrastructure Protection Task Force, or "IPTF"). The United States government also conducted exercises to assess the vulnerability of critical infrastructures in various departments, including the Department of Defense and Federal Bureau of Investigation. On May 22, 1998 the President issued Presidential Directive 63. That directive, among other things, organizes the United States economy and government into four horizontal sectors, each headed by a lead agency. Each sector is supposed to assess the level of vulnerabilities of its critical infrastructures and devise a plan to reduce those vulnerabilities, develop a system to identify and prevent major attacks and also develop a system to respond to an attack in conjunction with the Federal Emergency Management Agency ("FEMA").[53] The goal is to be able to protect United States' critical infrastructures from deliberate sabotage by 2003. Should sabotage occur after that date, the subsidiary objective is to ensure the effects would be "brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."[54]

At the heart of the United States' structure is the National Infrastructure Protection Centre ("NIPC"). The National Infrastructure Protection Centre is part of the Federal Bureau of Investigation and utilizes the resources of the Federal Bureau of Investigation's Computer Investigations and Infrastructure Centre ("CITAC"). The National Infrastructure Protection Centre's mandate is to conduct vulnerability analyses and to detect, deter, respond to and investigate unlawful intrusions into public or private networks. A sub-division of the National Infrastructure Protection Centre is

---

[52] Andy Scott.

[53] See speech notes for Michael A. Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Centre for appearance before the Senate Judiciary Committee on Technology, Terrorism and Government Information, (Washington, D.C.) June 10, 1998.

[54] Ibid.

FedCERT (Federal Computer Emergency Response Team), in effect a SWAT team for major cyber-terrorist attacks or network sabotage.[55] In 1997, FedCERT identified 2,300 "hits" (illegal penetrations or intrusions) on the networks under their supervision. In addition, many departments of the United States government have their own CERTS to counter an attack on their critical infrastructures.

Canada has no government organization equivalent to the National Infrastructure Protection Centre or FedCERT. In fact, Canada is one of the few information-intensive nations that is not part of FIRST, the Forum for Incident Response Teams. The Forum for Incident Response Teams is an international coalition of vulnerability analysts and computer incident response teams from governments as well as the private sector. There is in Canada, however, a private sector organization, CANCERT (the "Canadian Computer Emergency Response Team") that performs a role analogous to that of FedCERT. CANCERT was evidently established in an attempt to fill a vacuum left by government.

Each federal government department and agency has information technology security ("ITS") policy and procedures. The organizations within the security and intelligence community have particularly aggressive information technology security programs. The Communications Security Establishment and the Royal Canadian Mounted Police also co-chair the Interdepartmental Information Operations Working Group ("IIOWG") that shares information relating to threats to networks and discusses issues of mutual concern. The Communications Security Establishment, in its mandate to advise the federal government on the security aspects of its automated information systems, also has work underway that includes: developing a threat and vulnerability database; evaluating the threat posed by hacker tools and technologies; seeking partnerships with industry; developing and evaluating new security devices to thwart a cyber-attack; and discussing cooperation between Canada and existing CERT organizations. The Royal Canadian Mounted Police's Security Evaluation and Inspection Team ("SEIT") conducts security vulnerability services for government departments that include vulnerability analyses of computer systems. The Canadian Security Intelligence Service has designed its networks to be stand-alone and maintains its own ITS to respond to a major incident.

Committee Observations and Recommendations

In response to questioning by the Committee relating to Canada's preparedness to deal with attacks on our critical infrastructures as compared to the United States, the government witnesses stated that, while the United States is further advanced, Canada knows where it needs to go and it will get there. The Committee urges the government to develop the policies and provide the resources to allow us to get there as soon as possible.

---

[55] "The National Infrastructure Protection Centre: Working Together to Protect Our Nation's Critical Infrastructures", National Infrastructure Protection Centre, (Washington, D.C.) Undated; and United States Department of Justice News Release "Attorney General Unveils New Critical Infrastructure Protection Centre," (Washington, D.C.) February 27, 1998.

The Committee urges the government to give immediate and careful attention to the creation of a capability to assess and reduce vulnerabilities in critical infrastructures and to prevent or respond to physical and cyber-attacks. Because of the interconnected nature of our systems, the initiative should include both government at all levels and the private sector and should cover both public and private infrastructures. The Committee was impressed with the work done by the Department of National Defence to test the Canadian Forces networks. The Committee is concerned that this initiative appears to be confined to the one department. It should provide a template for a comprehensive program in which other departments and agencies test their networks in a cooperative and coordinated manner.

The Committee recommends that the Government consider providing for specific criminal offences and penalties under the *Criminal Code* to deal with cyber-attacks. At the present time, the most relevant section of the *Criminal Code* appears to be subsection 430(1.1) and 430(2), which provides:

> *(1.1) Everyone commits "mischief" who wilfully*
>
> *a) destroys or alters data;*
> *b) renders data meaningless, useless or ineffective;*
> *c) obstructs, interrupts or interferes with any person in the lawful use of data; or*
> *d) denies access to data to any person who is entitled to access thereto.*
>
> *(2) Everyone who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.*

Encryption

The expansion and increased reliability of the Internet have created an explosion in the growth of electronic commerce. Witnesses before the Committee cited sources that forecasted up to $350 billion (USD) in world-wide Internet-based electronic commerce by 2002.

The growth in electronic commerce and electronic communication brings with it a need to protect confidentiality and privacy. While most electronic communications and transactions are legal, terrorists and other criminal elements also use telecommunications and the Internet extensively and have a particular interest in safeguarding their communications from the prying eyes of government and security intelligence organizations. There are several techniques that have been available for some time to conceal information such as steganography, using obscure languages and "chaffing and winnowing".[56] The electronic encryption of communications and stored data, however, represents a

[56] "*Steganography*" means hiding a secret message within the body of a larger message so that a reader cannot easily discern the hidden message. "Chaffing and winnowing" in essence mean adding

quantum leap in the ability to conceal communications and data from third parties. Once the exclusive preserve of the military, encryption is now in the public domain through a range of encryption technologies.

Cryptography is vital to the growth of electronic commerce because it brings security to communications, provides for the encryption of databases and documents and provides for digital signatures to electronically authenticate messages and transactions. Cryptography technology also allows governments and security intelligence agencies to protect their sensitive communications. Cryptography obviously also creates challenges for law enforcement and security intelligence agencies in their ability to gain access to illegal or suspect communications or data; and the stronger the encryption technology used, the greater the challenges.

As indicated in Chapter I, in February, 1998 Industry Canada released a discussion paper on a cryptography policy framework for Canada. Within a broad policy framework on cryptography are three subsidiary issues: policies on the encryption of stored data, policies on the encryption of real-time communications, and export controls on encryption technology.[57] Industry Canada witnesses who appeared before the Committee indicated the policy framework considers a number of objectives, some of which are in competition or in conflict with each other. Those objectives include facilitating electronic commerce to promote economic development, protecting personal and commercial privacy and confidentiality, avoidance of a burdensome regulatory regime, promotion of the development of cryptography technology in Canada for the domestic market and for export and development of a cryptography legislative framework that allows for lawful interception by authorities for tax, law enforcement, security intelligence and other purposes.[58]

Witnesses who came before the Committee from the Royal Canadian Mounted Police and the Canadian Security Intelligence Service stated a very clear preference for a legislative or regulatory regime that provided them with mandatory access to the "keys" used to encrypt and decrypt communications and stored data. In August, 1997, the Canadian Association of Chiefs of Police issued a press release urging the federal government to adopt a mandatory key access system. Of the 18 law enforcement agencies that responded to the Industry Canada paper, each one supported mandatory key access.[59] Law enforcement and security intelligence agencies that appeared before the Committee and those that responded to the Industry Canada paper assert that they do not seek increased investigative capabilities through mandatory key access or otherwise, but instead seek only to restore and maintain their existing investigative capabilities.

---

useless or non-secret text to a message (i.e. chaffing) where the recipient uses a winnowing process (a secret authentication key using a standard message authentication code ("MAC") algorithm, to read or access the secret message.

[57] See Industry Canada, "A Cryptography Policy Framework for Electronic Commerce", op cit.

[58] A Bill to "support and promote electronic commerce" (Bill C-54) was tabled in the House of Commons on October 1, 1998 by the Minister of Industry.

[59] "Cryptography Policy Discussion Paper: Analysis of Submissions", prepared for Industry Canada by AEPOS Technologies Corporation, June 11, 1998 (unpublished).

Law enforcement and security intelligence agencies also seek legislative amendments, in particular changes to the *Criminal Code,* to compel the holder of a cryptographic key or password to give it up in response to a judicial warrant. The Canadian Association of Chiefs of Police has also asked for *Criminal Code* amendments to criminalize the use of cryptography in the commission of a crime.

From the responses to the Industry Canada paper it is clear, in numerical terms at least, that the law enforcement and security intelligence agencies are on the losing side of the debate over encryption. According to the analysis of the responses, 78% feel that there should be a lessening of controls over encryption.[60] The law enforcement and security intelligence agencies were alone in arguing for more control, namely mandatory key access. The majority view has clearly come down on the side of cost, economic development including facilitating the export of cryptography technology and on the side of privacy and confidentiality. A theme in many responses was a fear that the government would emphasize law enforcement and security intelligence requirements at the expense of privacy, cost, exports, economic growth and other considerations. As has happened in the United States, it now seems clear that any policy predicated on mandatory key access is not to be accepted in Canada.

In the absence of mandatory key escrow, law enforcement and security intelligence authorities will have to rely on technological and other solutions to break encrypted messages and stored data. Technological solutions will be very expensive, time-consuming and, in the case of strong encryption, in some cases ineffective. Problems exist even with a key escrow system in terms of real-time, or immediate conversion of encrypted messages into plain text.

Committee Observations and Recommendations

It is clear to the Committee that there is no perfect solution to balance the spectrum of interests that revolve around cryptography. Any attempt to develop a cryptography policy that balances law enforcement and security intelligence interests on one hand with commercial, economic development and privacy or confidentiality interests on the other hand presents a conundrum to policy-makers.

It is beyond the Committee's mandate and competence to suggest which approach to a cryptography policy is best. From testimony before the Committee it is clear, however, that the police and security intelligence agencies much prefer a mandatory key escrow system in order to maintain their

---

[60] With respect to encryption of stored data, 52% support a market-driven approach, 27% support no controls at all, 12% (all law enforcement/security intelligence agencies) support mandatory access and 6% support minimum standards. With respect to encryption of real-time communications, 43% support the status quo, 25% support no controls, 11% (all law enforcement/security intelligence agencies) support mandatory controls, 6% support placing obligations on the carriers and 5% supported other options, 12% explicitly objected to mandatory controls while supporting another option. With respect to export controls 88% supported a relaxation of controls, 6% favoured the status quo and 1% (a law enforcement agency) supported an extension of controls. (From "Cryptography Policy Discussion Paper: Analysis of Submissions," op cit.)

current position. It was equally clear from the evidence that a mandatory key escrow system is not likely to be adopted given all of the competing interests and issues. Therefore, the Committee urges the police and other agencies to actively investigate and explore other methods and techniques to address this very serious obstacle to intelligence-gathering and that government also consider other approaches, some of which the Committee understands are being considered by other countries.

Whatever the solution, the organizations within the security intelligence sector, namely the Canadian Security Intelligence Service and the Communications Security Establishment, will require additional resources to acquire the technology and to do the work necessary to maintain their current level of access to electronic communications and stored data. Even if a mandatory key access system were instituted, additional resources would be required, albeit of a smaller magnitude. The Committee was relieved to hear that, in the case of the Canadian Security Intelligence Service and the Communications Security Establishment, the incremental expenditures required for each would be in the "tens of millions" range annually, rather than the "hundreds of millions" range, or even higher. The Committee urges Industry Canada to include estimates of incremental costs for the Canadian Security Intelligence Service and the Communications Security Establishment in whatever policy proposals it makes to Cabinet.

The Committee also endorses recommendations to amend the *Criminal Code* to provide lawful access to encryption keys by law enforcement and security intelligence organizations and to criminalize encryption when used in the commission of a crime. The Committee also urges the law enforcement and security intelligence communities to consult with developers and suppliers of cryptography technology and with carriers and service providers so that each side may better understand the requirements and objectives of the other and, hopefully, arrive at mutually-agreed solutions.

Even should the encryption conundrum be effectively addressed from a security intelligence perspective, encryption is only one of a panoply of technological advances likely to affect, or having the potential to affect, the security intelligence community. Technology will continue to evolve and the security intelligence community will be on a technology treadmill in order just to keep up.

Nuclear, Biological and Chemical Weapons Attacks

As indicated in Chapter I, one of the new tactics available to terrorist groups is a range of nuclear[61], biological and chemical weapons. Authorities have assured the Committee that the actual direct and current threat to Canada and Canadians is low. Notwithstanding, recent incidents such as the release of Sarin gas in the Tokyo subway may have let the "genie out of the bottle" and acquainted terrorist groups with the power of nuclear, biological or chemical weapons.

---

[61] The risk of an incident involving nuclear weapons, per se, is very low. It is more likely that terrorists would use, or threaten to use, military or industry-grade plutonium or other radioactive materials and nuclear by-products to contaminate an area.

The United States government considers that the threat of a chemical or biological terrorist attack has increased in recent years.[62] The same degree of threat does not apply to Canada, although Canada could be a conduit for transporting nuclear, biological or chemical materials into the United States, or could be a venue for planning a nuclear, biological or chemical attack against the United States.

Experts in the security intelligence field suggest that because of their disdain for human life, the militant fringes of certain religious fundamentalist groups are most likely to mount a nuclear, biological or chemical attack. The United States has taken several initiatives to combat a nuclear, biological or chemical attack. The *Antiterrorism and Effective Death Penalty Act* (Title V) brings nuclear, biological and chemical weapons and materials within the ambit of United States' counter-terrorism legislation. Among other things, the United States legislation expands the scope of previous restrictions on the sale and use of nuclear substances, requires reports to Congress on any thefts of nuclear materials from United States military installations, and increases the penalties and controls pertaining to biological agents.

United States Attorney General Janet Reno has announced a federal organizational structure to counter the use of nuclear, biological and chemical weapons. That structure includes what has been called a "single window"[63] for state and municipal authorities to train first responders[64] and includes a commitment to buy appropriate equipment to counter a nuclear, biological or chemical incident. The *Antiterrorism and Effective Death Penalty Act* includes a long list of appropriations to fund training and equipment purchases and for a number of federal government departments and agencies to enhance their ability to monitor and control the movement of nuclear, biological and chemical materials. Those appropriations and others include $100 million (USD) to provide diagnostic, detection and protective equipment to local and state governments; a research program into gene mapping to trace and counter designer biological agents; and the development of a national stockpile of specialized medicines. The Secretary of Defence has also announced his intention to create and train up to 10 national guard units to be the second responders to a nuclear, biological or chemical incident.

The United States' approach to counter a nuclear, biological or chemical attack, albeit still largely on paper, consists of four levels. The first level is the segregation of United States territory into 120 metropolitan areas, each with an inventory of assets available to respond to a nuclear, biological or chemical incident and each with its specialized response strategy. The second level is enhanced coordination at the federal level and a single contact point for state and local authorities, including a national response capability. The third level is the detection and interception of biochemical precursors and equipment being shipped to rogue states or terrorist groups. The fourth level is deterrence of and response to those who would use a nuclear, biological or chemical weapon against

---

[62] **Antiterrorism and Effective Death Penalty Act**, subsection 2332c. (b) (1).

[63] "Clarke Previews New U.S. Steps to Counter Terrorism", **United States Information Service**, 8 October, 1998.

[64] The term "First Responders" refers to police, firefighters, ambulance attendants, etc. who would normally be first on the scene of any conventional or nuclear, biological or chemical incident.

United States citizens, installations or interests.

Canadian government witnesses before the Committee allowed that Canada lags behind the United States in planning for a nuclear, biological or chemical attack, but indicated that work is certainly underway in order to improve our defences and response capability. Centres of excellence[65] have been identified by Emergency Preparedness Canada and through the National Counter-Terrorism Plan that can be used to identify and help respond to the release of a biochemical substance. The inter-departmental Special Threat Assessment Group ("STAG")[66] exists in part to monitor trends and to help counter the use of nuclear, biological or chemical materials as weapons. Other initiatives taken include the Department of National Defence's development of a capability to respond to a nuclear, biological or chemical incident to assist local police forces and first responders; the Royal Canadian Mounted Police and the Department of National Defence have trained police explosive technicians in strategic areas across Canada in the detection and disarming of a nuclear, biological or chemical weapon; the creation of a Joint Nuclear, Biological and Chemical Response Team ("NBCRT") by the Royal Canadian Mounted Police and the Department of National Defence; development of specialized equipment for responding to a chemical or biological attack; and the training of first responders in containing and handling a nuclear, biological or chemical incident.

Although much has been accomplished at the federal level, the role that first responders play in an incident is critical. First responders are primarily employees of municipal services. First responders will (by definition) be first on the scene and will have to manage a nuclear, biological or chemical incident until help in the form of the Royal Canadian Mounted Police and the Department of National Defence arrives. Depending on the circumstances, help may be some time coming. Most municipal police forces and other first responders make no claim to having an effective response capability against a nuclear, biological or chemical attack.

The Committee heard from the National Capital First Responders' Committee. The First Responders' Committee is obviously aware of the nuclear, biological or chemical threat and is preparing to respond appropriately and effectively to a nuclear, biological or chemical incident. The Committee was also pleased to hear of the extensive cooperation between the First Responders' Committee and the Royal Canadian Mounted Police, the Department of National Defence and the Canadian Security Intelligence Service. The First Responders' Committee made it clear, however, that much more is required by way of equipment and training and inter-service coordination.

---

[65] "Centres of Excellence" include the Canadian Transport Emergency Centre (CANUTEC), the National Environmental Emergencies Centre, the Atomic Energy Control Board, the Laboratory Centre for Disease Control, the Defense Research Establishment Suffield (DRES) and the Special Threat Assessment Group (STAG).

[66] According to the National Counter-Terrorism Plan, the role of the inter-departmental Special Threat Assessment Group is to: "assess the nature, credibility and feasibility of a nuclear, biological or chemical terrorist threat; assess the short and long term consequences of the execution of such a threat; and recommend mitigating and preventative measures and advise on recovery measures to the Interdepartmental Policy Advisory Group (IPAG)."

Committee Observations and Recommendations

Although the risk of a nuclear, biological or chemical attack in Canada or against Canadian interests is low, much needs to be done in order to be able to respond properly should the unexpected happen. We must also guard against Canada being used as a conduit for nuclear, biological and chemical materials for terrorist purposes and also guard against Canada being used as a venue to plan or mount nuclear, biological or chemical attacks elsewhere. We require continuing development of technology to respond to a nuclear, biological or chemical attack. We need to ensure first responders receive the protective and diagnostic equipment they require in order to be able to perform mass decontamination, have available approved drugs for first responders and casualties and sufficient quantities of ventilators and hospital beds for mass casualties and to treat people with injuries who may also be chemically contaminated. We need regular joint training exercises among first responders, the Department of National Defence and the Royal Canadian Mounted Police. A national inventory should also be established of equipment and other assets that are available to respond to a nuclear, biological or chemical incident.

To the extent reasonably possible, the federal government should support the training of first responders across Canada. First Responders must be trained to identify a nuclear, biological or chemical incident and to respond appropriately. A conventional response to a nuclear, biological or chemical incident will increase the damage and thus play into the terrorists' hands. A model appears already to exist in the National Capital First Responders' Committee. The Senate Committee recommends that government encourage the proliferation of training and equipping of First Responders on the National Capital model or some enhanced version.

There is little that can be done to deny terrorists' access to basic chemical and biological weapons. Domestic laws or international conventions that restrict the export, manufacture and sale of certain explosives or explosive compounds are of little use in the fight against chemical and biological weapons. Such weapons can be made from easily accessible items and recipes for their manufacture are readily available on the Internet and from other public sources. Accordingly, the focus must be on intelligence to identify groups likely to use such weapons and their targets and on responding to and managing an actual incident.

The Government's Threat Analysis Capability

The terminology used within the security and intelligence community is often arcane and filled with mystifying acronyms such as SIGINT, MILINT, COMINT, HUMINT and the like. This makes comprehension and demystification of the security intelligence sector more difficult and also sometimes leads to misunderstandings by the public.

Within the Government of Canada four generic types of intelligence are collected:

Security intelligence is about activities that constitute a threat to the security of Canada. These

threats and the intelligence relating to them can come both within and from outside of the country. The Canadian Security Intelligence Service is the agency primarily responsible for the development of security intelligence.

Criminal intelligence refers to that information which the police should know in order to counter and apprehend those engaged in criminal activities. It is gathered primarily by law enforcement agencies and at the federal level by the Royal Canadian Mounted Police.

Military intelligence includes intelligence about military threats, capabilities, tactics and strategic assessments of future or potential military threats. Military intelligence is vital to Canada's peacemaking and peacekeeping commitments and to any incident where Canadian forces may be deployed, including the deployment of Joint Task Force Two ("JTF2")[67] in response to a terrorist incident. Military intelligence is the exclusive preserve of the Department of National Defence and the Communications Security Establishment.

Foreign Intelligence, at its broadest, is information about the capabilities, activities or intentions of foreign states, organizations or individuals. Usually, however, it is distinguished from security, criminal or military intelligence. It includes data of a political, economic, military, security, technological or social nature, obtained from overt as well as covert sources. Its purposes are to advance and facilitate the foreign policy process and to provide advantage in the pursuit or overall foreign policy objectives. The Department of Foreign Affairs and International Trade, the Department of National Defence, the Communications Security Establishment, the Canadian Security Intelligence Service and the Privy Council Office are each engaged, from time to time, in collecting, assessing or producing foreign intelligence.[68]

When the last Senate Special Committee on Terrorism and Public Safety reported in 1989, the then Department of External Affairs maintained a substantial foreign intelligence assessment (and threat analysis) capacity. With the end of the Cold War that capability has been substantially reduced. In fact, personnel were transferred to the Intelligence Assessment Secretariat of the Privy Council Office.

Distinctions between various categories of intelligence are sometimes blurred and the activities of the various organizations often intersect and are mutually supportive. The Privy Council Office plays a coordinating role and also continuously monitors the security and intelligence environment to identify emerging and evolving trends and to consolidate intelligence from multiple sources into a balanced, comprehensive view for the information of the Prime Minster, ministers and senior officials.

---

[67] JTF2 is the successor to the Royal Canadian Mounted Police's Special Emergency Response Team (SERT). See Report of the Senate Special Committee on Terrorism and Public Safety (1987) p.p. 63-68.

[68] The Intelligence Assessment Secretariat (IAS) at the Privy Council Office produces foreign intelligence assessments based on many sources. It does not collect raw intelligence.

Under the Committee's terms of reference, the Committee is to "examine and make recommendations with respect to the threat assessment capability of the Government of Canada relative to terrorism". The task is a difficult one. How does one evaluate a threat analysis capability when there is no "product" *per se*? How can a procedure that is conducted largely in secret for the exclusive use of a very limited number of very senior government officials and often relying on secret sources be evaluated by an outside authority? In such circumstances, the Committee's evaluation could only be done on a very macro, and perhaps superficial, level. Is there evidence that major terrorist threats to Canada have been missed or materially misapprehended by the Canadian security intelligence community?

On an on-going basis, the Canadian Security Intelligence Service is primarily responsible for threat analyses pertaining to terrorism. These can take a number of forms, from assessments of overall trends, to general assessments of particular targets or movements, to particular assessments about specific situations which have a threat potential.

The Canadian Security Intelligence Service has a comprehensive program of threat assessments (TAs) under which it prepares and disseminates to other Canadian government departments and agencies evaluations relating to specific threats – sometimes produced as a result of specific events (such as visits or meetings) but often as a result of requests from departments such as the Department of Foreign Affairs and International Trade or the Royal Canadian Mounted Police. These are usually time sensitive and deal with current intelligence, describing recent developments. The Coordinator of Security and Intelligence has characterized these threat assessments as "excellent, timely, clear and reliable". Furthermore, there is near-absolute consistency in the threat assessments made by the Canadian Security Intelligence Service and threat assessments made by provincial authorities and local police forces consulted by the Committee.

The Committee was, however, mainly concerned with the longer term and broader assessments produced by the Canadian Security Intelligence Service and others relating to real and potential threats to Canada's national security. As stated in Chapter I, Canada and Canadians have not been a major target for terrorist attacks over the past decade. There is nothing, therefore, to suggest that the security intelligence community has missed or misapprehended any threats. Furthermore, there is near-absolute consistency in the threat assessments made by the Canadian Security Intelligence Service and threat assessments made by provincial authorities and local police forces consulted by the Committee. Finally, there is a consistency in the Canadian Security Intelligence Service's international threat assessments with those of the United States, the United Kingdom and private and academic experts in the field of terrorism. Accordingly, there is no evidence to suggest that deficiencies exist in Canada's threat assessment capability *vis-à-vis* terrorism.

Several witnesses appeared before the Committee with suggestions as to how the threat assessment capability could be improved, however.

One concern was that the Canadian Security Intelligence Service makes less-than-optimal use of all the intelligence gathering assets spread across a range of departments and agencies of the Government of Canada. Many departments have their own "eyes and ears in the field", as well as

their own specialized expertise. Concern was expressed that these assets are not being fully used by, or integrated into, the threat assessment capability.

Chapter I referred to resource constraints and their impact on the security intelligence community. The Auditor General also noted that resources allocated to the community have declined significantly.[69] Should constraints on resources go too far, there will inevitably be negative repercussions on the community's threat analysis capability, in particular on its ability to respond to technological advances and on the ability of the Canadian Security Intelligence Service to collect security intelligence both within and outside of Canada.[70]

Evidence before the Committee indicated that there has been some re-allocation of resources by the Interdepartmental Committee on Security and Intelligence because of downsizing and changes in world conditions, so that the larger percentage of resources go to counter-terrorism and a smaller proportion into counter-espionage and other work. The Committee was informed that the Canadian Security Intelligence Service will continue to post liaison officers abroad who will share intelligence it generates in Canada and will continue to receive intelligence from foreign security intelligence and other intelligence services abroad.

There is concern, however, that Canada's needs may not always be given the priority they deserve by foreign security intelligence organizations and, furthermore, that the intelligence Canada receives may be filtered through the prism of other nations' domestic and foreign policies. There is also the concern that Canada's needs may not be satisfied if other nations' intelligence agencies retrench due to fiscal constraints, or if other nations withdraw from parts of the world due to changes in their national policies and priorities.

Canada relies on its allies for much of its security intelligence on international terrorists operating abroad. Although Canada itself faces little threat from terrorist violence, evidence indicates Canada is second only to the United States in the number of terrorists or potential terrorists organizations represented here. Accordingly, the careful monitoring of these terrorists or terrorist organizations by our security services provides a *quid pro quo* to our allies, particularly the United States.

In one particular area, the immigration screening area, there must be a careful balancing of information received from allied services. The McDonald Commission (1981) warned that,

> *"There is a danger in the immigrant screening process of putting too much faith and uncritical reliance on foreign agency information. The information received must always be carefully analysed in the context of the political circumstances of the country providing it. No foreign agency should be considered a "reliable source" in the sense that its reports can be accepted uncritically."* [71]

---

[69] Report of the Auditor General, op cit, para. 27.26.

[70] Pursuant to section 12, **Canadian Security Intelligence Service Act**, which has no geographic limitations on where the intelligence may be gathered.

[71] McDonald Commission, Second Report, Volume 2, p. 824.

More generally, reliance on friendly intelligence agencies may be problematic, or at least not sufficient, in the identification of regional and national trends and events that will impact on immigration flows to Canada. This reliance on foreign agencies informs the long standing debate as to whether Canada should expand its foreign intelligence capability. While Canada does not lack a foreign intelligence capability since "as noted earlier" several agencies are engaged in the collection and/or assessment and production of foreign intelligence, what Canada does lack is a single agency with a mandate to collect foreign intelligence overseas on an on-going basis. We do not have the Canadian equivalent of the Central Intelligence Agency in the United States or the British Secret Intelligence Service (BSIS or MI6) in the United Kingdom.

A related point raised before the Committee was Canada's reliance for intelligence on nations that reflect the World War II and Cold War alliance. Canada's closest intelligence allies are the United States, Britain, Australia and New Zealand. Although intelligence relationships are expanding, this expansion should be pursued aggressively so that we are not dependent on one particular perspective of the world.

Another concern raised is that the conduct of intelligence-gathering and analysis at the Canadian Security Intelligence Service may be driven by operational concerns and that threat analysis is performed by the Canadian Security Intelligence Service within an operational rather than an analytical mind-set. The Committee also heard proposals that the security intelligence community spend less resources on collection and more on analysis of intelligence. It was pointed out to the Committee that in today's information society there is almost a surfeit of information, mostly from open sources. Witnesses from the security intelligence community disputed this proposal pointing out that much of the information is not necessarily reliable, nor necessarily germane to Canada's interests and often becomes available after an event or after the subject becomes topical. A final concern expressed by one witness before the Committee is that the coordination of intelligence gathering, analysis and assessment by the Privy Council Office reflects a management orientation rather than a strategic one.

Committee Observations and Recommendations

The previous Special Committees on Terrorism and Public Safety raised issues about the federal government's (particularly the Canadian Security Intelligence Service's) threat assessment capability relating to terrorism. In the past, the Canadian Security Intelligence Service and the security intelligence community as a whole appeared to have missed, or at least underestimated, the threat in several instances.

Because the Committee did not have access to review or analyse any past or present threat assessments prepared by the security intelligence community, the Committee does not have the best evidence upon which to make an objective evaluation of the government's current threat assessment capability. There is, however, no evidence of deficiencies or other problems that came to the Committee's attention. The Committee is of the view, however, that such an evaluation should be

done periodically by an objective authority that has full access to the gamut of threat assessments prepared by the community (See Chapter IV).

With increasing globalization, dramatic changes in the tools and tactics available to terrorists, the changing political climates throughout the world and Canada's active international role and interests, the Committee believes there will be a growing need and demand for foreign intelligence. In the past, Canada has met its needs without taking the step of creating an intelligence service whose sole function would be to operate outside of our country's borders. Indeed, the fact that Canada does not have a separate foreign intelligence agency may have served us well in our role as a moderate power broker. To create such a new agency would create a different international image and would change Canada's perceived "neutral role" in many international forums. On balance, the Committee believes that this continues to be the appropriate and the most effective position for our country.

However, in the absence of a foreign intelligence service, the challenge for Canada will be to meet the increasing need and demand for relevant foreign intelligence. Much can be done through existing mechanisms. For example, existing bilateral and multilateral relationships should be continuously re-examined within an evolving climate. Canadian foreign service officers and other Canadian employees working abroad should be refocused to ensure that their information capabilities are working optimally to meet Canada's evolving needs. Our effectiveness in improving our foreign intelligence capabilities will largely depend upon increasing the level of cooperation and coordination that can be brought to bear both within the security and intelligence community and in the wider government sphere.

Canada needs a more strategic orientation to the collection, analysis and production of foreign intelligence. Therefore, the Committee strongly urges the Government to ensure that adequate and appropriate resources: policy, financial and personnel, be directed to this important task. This appears to be an appropriate role for the Privy Council Office to ensure that maximum use is made of all existing intelligence sources from across the Government of Canada. While the Committee is not recommending at this time the creation of a separate foreign intelligence service, we do not rule it out. The Committee views this option as a last resort to be considered in the future should efforts to improve the current situation prove to be inadequate to meet our country's total intelligence requirements.

Parliament's Role and Responsibility

An overarching assumption made in Canada is that "intelligence" including security intelligence is exclusively for the administrative branch of government. With very few exceptions, Parliament is not part of the loop in terms of receiving intelligence analyses or assessments generated by the intelligence community. In our system, the consumers of intelligence have been limited to policy makers and decision makers within the executive branch of government. Parliament, in being asked to approve legislation, budgets and policy initiatives, is largely deprived of direct access to any intelligence analyses or assessments.

For example, in discussion of proposed legislation to address money laundering, should not parliamentarians be fully briefed on the security intelligence that helped identify the problem and the proposed solution? During the forthcoming review of the *Immigration Act*, should not parliamentarians have access to security intelligence to help assess how effective the Act will be in addressing valid security concerns? Would parliamentarians not have a better understanding of domestic and international developments and the Government of Canada's response if they had reasonable access to foreign intelligence analyses? Access to intelligence would also allow parliamentarians to gauge its value, accuracy and timeliness.

According to a study on information-sharing between Congress and the intelligence community in the United States,

> "*...intelligence has made Congress a smarter, more effective critic of the executive branch, often complicating the lives of policy officials.*"[72]

Therein, perhaps, lies the answer. As long as the administrative branch has a monopoly on intelligence it exercises a distinct advantage over Parliament.

Committee Observations and Recommendations

The Committee recommends that the security intelligence community explore ways by which parliamentarians may be brought at least partially into the intelligence loop without prejudicing national security. Obviously, Parliament cannot and need not have access to all, or the most sensitive, national security information, all of the time.

In this regard, the Committee proposes regular briefings for parliamentarians on security issues and trends and accommodating parliamentarians' requests for briefings on specific issues.

---

[72] Brett Snider, "Sharing Secrets With Lawmakers: Congress as a User of Intelligence", Library of Congress, Washington, D.C., February 1997.

CHAPTER IV

LEADERSHIP, COORDINATION, REVIEW AND OVERSIGHT OF CANADA'S SECURITY AND INTELLIGENCE COMMUNITY

Overview

Although small relative to the establishments of other G8 nations, the eleven core organizations, additional organizations on the periphery and the complex of interdepartmental committees that constitute Canada's security and intelligence community account for approximately one-half billion dollars in annual operating expenditures. In this light, the Committee reviewed the extent to which leadership and coordination exists within the community to avoid duplication of effort and to ensure the community pursues objectives and priorities that reflect each organization's mandate and Canada's policies and interests. Furthermore, many of the organizations within the security and intelligence community exercise invasive powers that impact, or have the potential to impact, on personal rights and freedoms.[73] In a country such as Canada, it is important that these powers be subject to some form of review to ensure they are being exercised in accordance with the law and the rules of natural justice. It is also important that people who feel aggrieved by the exercise of such powers have recourse to an independent review.

Currently, there are independent review or oversight bodies for the Canadian Security Intelligence Service, the Communications Security Establishment and the Royal Canadian Mounted Police. In addition, the Auditor General has the authority to conduct broad scope audits of any department and agency of the federal government and has conducted an audit of the Canadian security intelligence community. Specific recourse is also available through the Access and Privacy Commissioners and through statutes such as the *Canadian Human Rights Act* and the *Privacy Act*. Judicial review applies to the actions of the organizations within the security and intelligence community under the *Canadian Charter of Rights and Freedoms*, or as specifically provided for in individual statutes (e.g. the *Canadian Security Intelligence Service Act*). Although important, judicial review is not included within the ambit of "review" or "oversight" for purposes of this Report.

Another area of study for the Committee was the extent to which Canada's security and intelligence community is, or should be, subject to some form of parliamentary review or oversight.

---

[73] Such as the Canadian Security Intelligence Service, the Communications Security Establishment, the RCMP, Revenue Canada (Customs and Excise), Citizenship and Immigration Canada.

A Word on Terminology

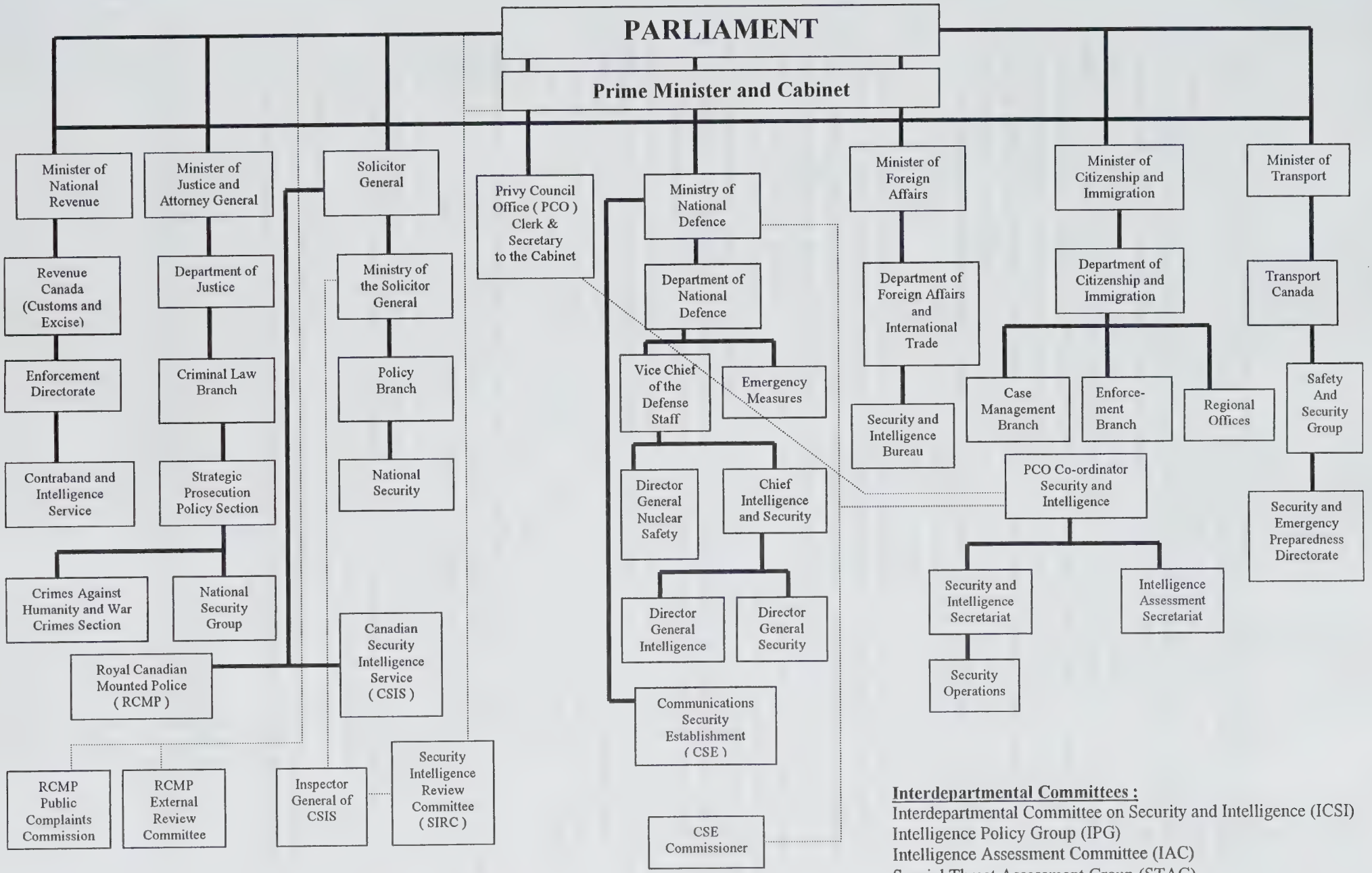
The terms "review" and "oversight" are often confused when used in the context of security and intelligence. For purposes of this Report the Committee has defined "Review" as the post-facto audit of actions taken or policies pursued by a security or intelligence organization. Although they may make recommendations, review bodies rarely have the authority to impose their will aside from whatever powers of moral suasion they can muster. "Oversight" bodies on the other hand exercise some on-going control over the policies, procedures and activities of the agencies for which they are responsible. Review and oversight bodies can exist in either or both the administrative and legislative branches of government.

Leadership and Coordination

The Committee was impressed by the substantial progress that has evidently been made in leadership and coordination of the security and intelligence sector since the last Special Committee on Terrorism and Public Safety reported in 1989.

Leadership and coordination are currently conducted within the administrative branch and operates at two levels. One level is on-going, day-to-day leadership and coordination of the community. The other level is leadership and coordination of the community during an actual security incident.

Table 5



Interdepartmental Committees :

Interdepartmental Committee on Security and Intelligence (ICSI)
Intelligence Policy Group (IPG)
Intelligence Assessment Committee (IAC)
Special Threat Assessment Group (STAG)

*** Source : Privy Council Office and Committee Research**

On-Going Leadership and Coordination

Table 5 illustrates in schematic form the security and intelligence community within the Government of Canada and the leadership and coordination infrastructure for the federal security and intelligence community. The pivotal role in this infrastructure is played by the Privy Council Office. This role is entirely appropriate given that the Privy Council Office is the Prime Minister's department as well as the Cabinet secretariat. Ultimately, the Prime Minister is responsible for the security of Canada. Given the number of departments and agencies with responsibilities for security and intelligence, it is not only appropriate, but also necessary that the Privy Council Office assist the Prime Minister in setting the priorities for the entire security and intelligence community within the federal Government and then monitoring and co-ordinating the activities throughout the community to ensure that those priorities are met.

The previous Senate Special Committees on Terrorism and Public Safety noted that the Cabinet Committee on Security and Intelligence had fallen into disuse and it rarely, if ever, met. Those Committees expressed concern, therefore, that there was no active, formal mechanism by which the Prime Minister and Cabinet exercised on-going control, direction and accountability over the security and intelligence community. The Cabinet Committee on Security and Intelligence no longer exists, even on paper. Instead the Ministers Meeting on Security and Intelligence ("MMSI") chaired by the Prime Minister[74] meets as needed and at least once each year. The essential function of the Ministers Meeting on Security and Intelligence is to establish priorities for the security and intelligence community, meaning the foreign and defence intelligence priorities as well as the national requirements for security intelligence. Ministers may also meet on an *ad hoc* basis at the call of the Prime Minister when specific policy or operational issues arise pertaining to the security and intelligence sector. The Cabinet Committee on the Social Union has also been designated as the forum for the discussion of security and intelligence issues that arise in the context of broader policies.

Beneath this political overlay is the bureaucratic coordination infrastructure, either housed within the Privy Council Office in the form of secretariats, or conducted by interdepartmental committees, the most important of which are chaired by officers of the Privy Council Office. Within the Privy Council Office is the Security and Intelligence Coordinator, supported by the Assistant Secretary, Security and Intelligence Secretariat. The Secretariat monitors and coordinates the community on a day-to-day basis within the framework of policies and priorities established by the Ministers Meeting on Security and Intelligence.

The most important interdepartmental committee for the security and intelligence community is the Interdepartmental Committee on Security and Intelligence ("ICSI"). The Interdepartmental

---

[74] The Vice-Chair is the Deputy Prime Minister, the members are the Minister for Foreign Affairs, the Minister of National Defence, the Solicitor General and Minister of Justice, plus other Ministers who may be invited by the Prime Minister.

Committee on Security and Intelligence is a deputy minister level committee chaired by the Clerk of the Privy Council and Secretary to the Cabinet. It reviews major policy, resource and operational proposals relating to security and intelligence being made to Cabinet, advises the Ministers Meeting on Security and Intelligence on priorities for the community and considers major intelligence issues.[75]

The Interdepartmental Committee on Security and Intelligence Executive Committee is chaired by the Coordinator, Security and Intelligence and meets as required, but more frequently than the Interdepartmental Committee on Security and Intelligence, to ensure senior officials' attention to key policy, operational and resource issues impacting on the community as they arise.

The Intelligence Policy Group ("IPG") is an assistant deputy minister level committee chaired by the Assistant Secretary to the Cabinet, Security and Intelligence. It meets bi-weekly and is the principal forum for policy and operational coordination within the community.

The Intelligence Assessment Committee ("IAC") also plays a coordination role. Its function is to provide analytical reports and assessments to the Prime Minister, Ministers and senior officials based on intelligence and other contributions from a number of organizations within the community and from elsewhere.

Unlike the United States[76], for example, there is no single resources envelope for the security and intelligence community within the Government of Canada. Each organizational element of the community is part of individual envelopes that correspond to individual ministerial portfolios. The Coordinator, Security and Intelligence, helps to manage and negotiate within the sector to ensure resources are sufficient to meet identified priorities and objectives. The Coordinator will also bring any resource issues to the attention of Cabinet for resolution.

In addition, the Treasury Board Secretariat is a member of the Interdepartmental Committee on Security and Intelligence and the Treasury Board representative is invited to attend the Interdepartmental Committee on Security and Intelligence Executive Committee meetings when major resource proposals or issues are on the agenda. As part of its normal mandate, the Treasury Board examines departmental expenditure proposals relating to security and intelligence programs.[77]

As indicated earlier, the Canadian security and intelligence community is relatively small. Government witnesses told the Committee that this allows for, and indeed encourages, an "inherent

---

[75] Over the past year, items on Interdepartmental Committee on Security and Intelligence's agenda have included security at the APEC Summit, cryptography policy and its implications for the sector, and the protection of critical infrastructures from threats.

[76] See Johnston, L.K and Sheid, K.J, "Spending for Spies: Intelligence Budgeting in the Aftermath of the Cold War", **Public Budgeting and Finance**, Winter, 1997, p.p. 7-26.

[77] Letter to Committee Chair from Margaret Purdy, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office (September 25, 1998).

cohesion" that is impossible in larger security and intelligence communities. In addition to the formal interdepartmental structure, therefore, there exists a complex of interpersonal and professional relationships and communication links.

Government witnesses before the Committee testified that the coordination mechanisms work well and the spirit of cooperation and attention to security and intelligence matters have increased substantially since the last Senate Special Committee on Terrorism and Public Safety reported.

One of the issues raised by both previous Special Committees on Terrorism and Public Safety was the lack of cooperation between the Royal Canadian Mounted Police and the Canadian Security Intelligence Service. This lack of cooperation existed at all levels: from a failure to communicate an actual threat in the case of a Punjabi Cabinet Minister visiting Canada, to the inability of the Canadian Security Intelligence Service to access the Canadian Police Information Centre ("CPIC"), because, in the words of the Royal Canadian Mounted Police, "the Canadian Security Intelligence Service is not a police organization". The Special Committees were not impressed with this explanation and characterized it as a "turf battle."

Coordination and cooperation between the Royal Canadian Mounted Police and the Canadian Security Intelligence Service appear to have substantially improved. Memoranda of Understanding between the Royal Canadian Mounted Police and the Canadian Security Intelligence Service are now in place on the exchange of liaison officers across Canada and on the sharing of intelligence and, according to witnesses, the Royal Canadian Mounted Police and the Canadian Security Intelligence Service openly share threat assessments on events and visits involving Internationally Protected Persons ("IPP's"). The Canadian Security Intelligence Service has also been granted access to the Canadian Police Information Centre by virtue of a Memorandum of Understanding.

The Committee suggests that a similar agreement be entered into to allow the Canadian Security Intelligence Service access to the Violent Crime Linkage Analysis System ("ViCLAS"). The Violent Crime Linkage Analysis System is a national computer-based system set up by the Royal Canadian Mounted Police and linking all major police forces in Canada. It is designed to disseminate profiles of crimes and criminals in order to assist in linking crimes committed in different police jurisdictions.

Coordination During A Security Offences Incident

Terrorist and other security offences occur often without warning and can vary enormously in terms of intensity, the length of time for the incident to play out, international implications, the nature of the threat and the appropriate response. It is, therefore, impractical to have a hard and fast "rule book" of who does what, when and how in response to an actual incident. Coordination protocols and mechanisms can and should, however, be in place and be periodically tested and updated.

For domestic terrorist incidents, the Solicitor General is the "lead Minister" supported by his Ministry, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the

interdepartmental infrastructure. For incidents involving Canadians or Canadian interests outside of Canada, the Minister of Foreign Affairs is designated the lead Minister for purposes of the Government of Canada's response. It is recognized by all concerned that circumstances may compel the Prime Minister (or his designate) to assume responsibility for the government's response to a particular incident.

The coordination mechanisms and protocols for responding to a terrorist incident are set out in the National Counter-Terrorism Plan ("NCTP"). The National Counter-Terrorism Plan and the Committee's observations and recommendations concerning it are contained in Chapter II.

Committee Observations and Recommendations

From testimony before the Committee and from all other evidence available to the Committee, substantial progress has clearly been made in enhancing central coordination and leadership of the security and intelligence community. The Auditor General concluded that, "Substantial arrangements for control and accountability are in place, and progress has been made in recent years in strengthening them."[78] For that progress, the government and the officials involved deserve praise. The Committee would like to make a few observations.

The Committee welcomes the new Ministers Meeting on Security and Intelligence.[79] Since January 1, 1997 there have apparently been six sessions of this group, or *ad hoc* meetings of ministers on security and intelligence. The previous Senate Special Committees were concerned to note the effective demise of the Cabinet Committee on Security and Intelligence. It is crucial that there be a formal process for the Ministers in the security and intelligence community to set the foreign intelligence, military intelligence and security intelligence priorities to guide all the activities of the sector in collection, assessment and production of intelligence. This is the role now fulfilled by the Ministers Meeting on Security and Intelligence. The Committee also heard that there is a marked improvement from a decade ago in the attention given to these issues, including at these very high levels. Given the sensitivity and importance of the activities conducted by the security and intelligence community, the Committee believes this kind of effective political control, direction and accountability is absolutely essential.

While coordination of policies and priorities appears to be effective, the Committee is concerned about the coordination of resource allocation. Government witnesses before the Committee concentrated on the coordination of policies and priorities, but gave much less attention in their testimony to the coordination of resources. The Committee suggests the government examine the feasibility and value of a single security and intelligence envelope as well as the value of instituting a greater role for the Ministers Meeting on Security and Intelligence in resource allocation. This would enhance Cabinet's ability to avoid duplication, conflict and gaps in activities and to add

---

[78] Auditor General's Report, op cit, para. 27.5.

[79] Letter to the Committee Chair from Margaret Purdy, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office, (September 25, 1998).

leverage to the coordination of polices, priorities and operation.

The Committee acknowledges that the Canadian security and intelligence community is relatively small and (at least in expenditure terms) is dominated by three organizations: the Canadian Security Intelligence Service, the Communications Security Establishment and the Royal Canadian Mounted Police. The Committee also acknowledges that informal coordination mechanisms are both inevitable and valuable. Notwithstanding, informal mechanisms are a poor substitute for formal ones in the security and intelligence sector. The sensitivity and importance of the activities conducted require unambiguous and transparent lines of authority as well as unambiguous lines of communication, direction, control and accountability.

Finally, the Committee believes it would be valuable to identify both formally and publicly the group of organizations or parts of organizations that constitute the federal security and intelligence community. **Table 5**, in this Report, is a start. The Committee notes that this has been done in the United States through Presidential Executive Order[80] and, in the United Kingdom, by legislation.[81] This will be discussed in more detail later on in this Chapter.

Oversight and Review of the Security and Intelligence Sector

Formally-constituted review mechanisms exist only for three organizations within the security intelligence community: The Canadian Security Intelligence Service, the Communications Security Establishment and the Royal Canadian Mounted Police. This Committee has examined the review mechanisms of the first two of these organizations.[82]

The Canadian Security Intelligence Service has two review bodies, one "internal", the other "external". In corporate parlance, the former is akin to the internal auditor; the latter is akin to the external auditor. The Security Intelligence Review Committee (the external review body) is

---

[80] Executive Order 12333 (1981).

[81] The Intelligence Services Act, 1994.

[82] The Royal Canadian Mounted Police Public Complaints Commission was established in 1986 under the Royal Canadian Mounted Police Act. The function of the Commission is to review public grievances while ensuring that complaints are dealt with individually and fairly for both the public and members of the Royal Canadian Mounted Police. The Commission is comprised of a Chairman, a member for each province and territory that contracts with the Royal Canadian Mounted Police for policing services and up to three other members. All members of the Commission are appointed by the Governor-in-Council. Grievances and appeals by members of the Royal Canadian Mounted Police can be made to the External Review Committee which acts as one level of a two-level review process. It hears grievances and complaints and submits recommendations to the Commissioner of the Royal Canadian Mounted Police who acts as the second and last level of review. The External Review Committee is comprised of a Chairperson, a vice-Chairperson and three members. Because its mandate includes only members of the Royal Canadian Mounted Police, it is not considered a "review body" for purposes of this Report.

established under the *Canadian Security Intelligence Service Act.*[83] It is comprised of three to five people (including the Chair) appointed by the Governor-in-Council. Appointees to the Security Intelligence Review Committee must be Privy Councillors.

The Security Intelligence Review Committee's role as set out in section 38 of the *Canadian Security Intelligence Service Act* is to review generally the performance by the Canadian Security Intelligence Service of its duties and functions. The Security Intelligence Review Committee's role includes: conducting investigations of public complaints, reviewing reports of the Director of the Canadian Security Intelligence Service and the Inspector General, reviewing ministerial directives to the Canadian Security Intelligence Service, conducting investigations into reports submitted to the Security Intelligence Review Committee under the *Citizenship Act*, the *Immigration Act* and the *Canadian Human Rights Act* and reviewing complaints springing from denial of security clearances. The results of investigations of public complaints are reported to the complainant, the Minister and Director and, in the case of denials of security clearances, to the complainant and the deputy minister of the department concerned. In addition, the Security Intelligence Review Committee must make an annual report to the Solicitor General that is tabled in Parliament. The Security Intelligence Review Committee may, at the Solicitor General's request or at the Security Intelligence Review Committee's own initiative, prepare special reports for the Solicitor General "concerning any matter that relates to the performance of its duties and functions." [84]

The Inspector General (the "internal" review body) is also established under the *Canadian Security Intelligence Service Act.* The incumbent is appointed by the Governor in Council and reports to the Solicitor General. The mandate of the Inspector General is to monitor compliance by the Canadian Security Intelligence Service with its operational policies, to review the Canadian Security Intelligence Service's operational activities and to submit certificates to the Solicitor General confirming that the Canadian Security Intelligence Service has conducted its activities lawfully and without unreasonable or excessive exercise of its powers.

Both the Security Intelligence Review Committee and the Inspector General have unrestricted access to information generated or retained by the Canadian Security Intelligence Service. Both the Security Intelligence Review Committee and the Inspector General indicated complete satisfaction to this Committee that their access rights are respected by the Canadian Security Intelligence Service.

The relationships between the Canadian Security Intelligence Service and its review bodies appear to be working well, although there appears to be some tension between the Security Intelligence Review Committee and the Canadian Security Intelligence Service. Such tension is perhaps both understandable and reassuring given the Security Intelligence Review Committee's mandate.

The Commissioner for the Communications Security Establishment was appointed in 1996 under the *Inquiries Act* for a period of three years. A resolution to create the post was passed in the House of

[83] Section 34.
[84] Section 54.

Commons. Although one would expect the review function to be extended when the current Commissioner's term expires, there is no obligation, or commitment by the government, to do so. The Communications Security Establishment Commissioner investigates whether the Communications Security Establishment operates in compliance with the law.[85] The Commissioner decided, however, not to review complaints pertaining to actions that took place prior to his appointment.[86] The Commissioner may not investigate any matter for which other avenues of redress exist by statute. The Commissioner may report to the Minister for National Defence and, on a case-by-case basis, may also report to the Attorney General of Canada. Each year the Commissioner submits a general report to the Minister of National Defence for the Minister to table in Parliament. The Commissioner consults with the Privy Council Office on any report (including his reports to the Minister) to ensure they contain no information that prejudices the security of Canada or intelligence sources. When the Commissioner investigates a complaint from a member of the public, the Commissioner may report his findings only to the Minister, not to the complainant. In his testimony before the Committee and in his Annual Report (1997-98) the Commissioner declared this situation unsatisfactory.

Also in his testimony and in his annual reports, the Communications Security Establishment Commissioner recommended that a permanent review body for the Communications Security Establishment be created by statute with a wider mandate than that of the Commissioner. More will be said of these recommendations later on in this Chapter.

Committee Observations and Recommendations

Review or oversight of all the organizations that constitute Canada's security and intelligence community and the community as a whole is underdeveloped. In the Committee's view, the activities of the community demand effective, broad scope review. In the case of the Communications Security Establishment, the Senate Committee strongly supports the Communications Security Establishment Commissioner's recommendation that the Communications Security Establishment be given a statutory base and that the statute also provide, for a permanent review body.

The Security Intelligence Review Committee model has much to commend it in terms of legislative base, mandate, organization and powers for purposes of review. Accordingly, the Senate Committee proposes that the Security Intelligence Review Committee model be used for the Communications Security Establishment. This begs the question as to whether the mandate of the Security Intelligence Review Committee should be extended to include the Communications Security Establishment, or whether a new "Security Intelligence Review Committee-like" review body should be set up for the Communications Security Establishment.

---

[85] The original wording of the Motion was to have the Security Intelligence Review Committee undertake the review function. This was subsequently amended to refer to a "Security Intelligence Review Committee-like" review.

[86] Communications Security Establishment Commissioner, **Annual Report**, 1997-1998, p. 9

An argument was made before the Committee that the differences among organizations requires that the Canadian Security Intelligence Service and the Communications Security Establishment must each have its own review body. A concern was also expressed to the Committee that having a single review body would concentrate too much sensitive information in one organization or group of people. On the other hand, representatives of the Security Intelligence Review Committee felt that efficiencies could be gained by having the Security Intelligence Review Committee as the review body for both organizations. On balance, the Senate Committee proposes that a new review body be established by statute for the Communications Security Establishment.

The Committee did not study each organization within the security and intelligence community to the point required to recommend whether each required a review mechanism, or the type of review mechanism appropriate in each case. However, as a general principle, there should be a review mechanism for any organization with a security intelligence mandate that exercises powers that impact on the privacy and other civil rights of Canadians. The Committee urges the government to study the feasibility of creating one or more review bodies for the remaining organizations within the federal government's security and intelligence community.

Parliamentary Review and Oversight

The essence of Parliament's role in the British constitutional system is to act on legislative proposals made by the Ministry, to control public expenditures and to hold Ministers to account, both collectively and individually, for the exercise of their ministerial powers and for the general administration of their departments. In addition, Parliament exercises certain powers of administrative review, such as the review of regulations and other statutory instruments, which in Canada is done through the Standing Joint Committee of the Senate and the House of Commons for the Scrutiny of Regulations ("SJC").

The Canadian Security Intelligence Service was the first security intelligence agency in the federal government to be established by statute and to have a statutory review body. The *Canadian Security Intelligence Service Act* is still the standard in terms of statutory framework, the review mechanism itself and accountability linkages through the Solicitor General to Parliament.

It is perhaps instructive to review some history at this point, in particular how the McDonald Commission (which recommended the creation of a civilian security intelligence agency) and the government-of-the-day sought to balance external review, including parliamentary review, with the exigencies of a security intelligence operation. The McDonald Commission recommended that the Canadian Security Intelligence Service be established by an Act of Parliament, that the Minister have sufficient knowledge of the Canadian Security Intelligence Service's activities in order to properly account to Parliament and that a joint parliamentary committee be established in order "to scrutinize (the Canadian Security Intelligence Service's) activities with a view to ensuring that it fulfills the intentions of Parliament as set out in the organization's legislative charter".[87]

[87] McDonald Commission, Second Report, Volume 2, p. 899.

The McDonald Commission's recommendations concerning the role of the Minister were implemented. Subsection 6(1) of the *Canadian Security Intelligence Act* specifies that the Director is responsible for the control and management of the Canadian Security Intelligence Service, but "under the direction of the Minister" and that both the Security Intelligence Review Committee and the Inspector General report to the Minister. This accomplishes the McDonald Commission's objective of having Ministers

> *"...possess the knowledge to answer questions about security intelligence activities... They may choose not to divulge in public some of the information which they have, but such non-disclosure will be of their own choosing and not because the information is kept from them by the security organization."* [88]

Such a linkage is critical if Ministers are to be held accountable to Parliament.

McDonald's recommendations relating to a joint Senate and House of Commons committee of Parliament were not implemented. Instead, there were several compromises to recognize a role for Parliament in reviewing the Canadian Security Intelligence Service's operations.[89] One was to require the Security Intelligence Review Committee to report annually to both Houses of Parliament. Such reports could contain whatever recommendations for "changes" the Security Intelligence Review Committee might propose. The second was the five year review entrenched in the *Canadian Security Intelligence Service Act*. Another was the requirement under the Act that the Prime Minister must consult with the leader of each official party in the House of Commons on proposed appointments to the Security Intelligence Review Committee. Another was the statutory requirement under subsection 34(1) of the Act that appointees to the Security Intelligence Review Committee must be Privy Councillors. The objective of the latter was to have experienced, known parliamentarians who could act, and be seen and accepted as acting, as almost a surrogate for Parliament in the review of the Canadian Security Intelligence Service and who could also better understand and respond to the requirements and prerogatives of parliamentarians. In the event, successive governments have ignored the intent of this compromise by making most of the appointees Privy Councillors just prior to their appointment to the Security Intelligence Review Committee.[90] Of the eleven people appointed to the Security Intelligence Review Committee since

---

[88] Ibid., p. 896, para. 34.

[89] During debate on the Bill to create the Canadian Security Intelligence Service and the Security Intelligence Review Committee, the then Solicitor General, Robert Kaplan, M.P. stated "So even with the rejection of the McDonald Commission's recommendations about the permanent review committee...this legislation does contemplate greater parliamentary review in a way that is not controlled by the Solicitor General."

[90] Committee member, Senator LeBreton, was responsible for co-ordinating senior appointments in the Prime Minister's Office from 1984-1993. It is her recollection that it was very difficult to find Privy Councillors who were both qualified and interested in being appointed to the Security Intelligence Review Committee. As a consequence, the Mulroney government adopted the expedient of appointing

its establishment, only two (Hon. Ronald Atkey and Hon. Jean-Jacques Blais) were already Privy Councillors.

In the security and intelligence community only one organization, the Canadian Security Intelligence Service, has been established by an Act of Parliament. The Communications Security Establishment was transferred to the Department of National Defence for administrative purposes in 1975 through an Order-in-Council under the *Public Service Rearrangement and Transfer of Duties Act.*[91] Other elements of the community have been set up administratively within departments and agencies, or by inter-departmental administrative arrangement. The Committee suggests, however, that because of the importance and sensitivity of the activities they conduct, a special type of accountability is required.

Section 56 of the *Canadian Security Intelligence Service Act* called on Parliament to establish a committee, after the Act had been in force five years, to undertake "a comprehensive review of the provisions and operation of the Act." This review was conducted by a Special Committee of the House of Commons, which tabled its report in September, 1990.[92] The government of the day intended to conduct another review in 1998. The current government has yet to follow through on that commitment. The Committee also notes that the House of Commons Standing Committee on Justice and the Solicitor General established the Sub-Committee on National Security in the 34th Parliament. The Sub-Committee has not yet been re-established in the current Parliament.

Upon completion of the five-year review, the Special Committee and its Chairman and Director of Research expressed dissatisfaction with the review, in particular with their inability to obtain from the Canadian Security Intelligence Service, the Security Intelligence Review Committee, or the Inspector General the information that they considered necessary to perform the review as required by the statute. Among its recommendations, the Special Committee proposed the creation of a permanent sub-committee (of what was then the House of Commons Standing Committee on Justice and the Solicitor General) as the parliamentary review body for the security and intelligence sector.

The Special Committee was very clear that its intention in making this recommendation was **not** to impose an additional level of review on the Canadian Security Intelligence Service; rather, it was seeking to oversee the activities of the Security Intelligence Review Committee and the Inspector General - to watch the watchers. The Committee Report stated:

---

persons Privy Councillors for purposes of their appointments to the Security Intelligence Review Committee. The current government has continued that practice.

[91] PC 1975-95 (January, 1975) transferred the Communications Branch of the National Research Council of Canada to the Department of National Defence effective April 1, 1975. Other Orders-in-Council were issued pertaining to the management and administration of the "Communications Security Establishment" as the relocated agency was to be named (PC 1975-685, PC 12975-686, PC 1975-708, PC 1975-709).

[92] Report of the Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act, **In Flux but not in Crisis**, Ottawa: Queen's Printer, 1990.

"The Committee is also cognizant of the fact that the review process places burdens on organizations that are subject to review. It therefore wishes to be particularly careful not to impose on agencies such as the Canadian Security Intelligence Service an additional level of review. The Committee has already recommended that the Security Intelligence Review Committee should normally request the Inspector General of the Canadian Security Intelligence Service to conduct compliance reviews. The Committee is not recommending that the [proposed] sub-committee's research staff have a function similar to those (sic) of the Security Intelligence Review Committee or the Inspector General. Nor does it believe that the sub-committee would ask the Canadian Security Intelligence Service for information frequently. Such matters would be addressed through the Security Intelligence Review Committee. Rather the Committee believes that the sub-committee's role would be primarily three-fold. First, it would review budgets and make recommendations concerning the Main Estimates to the Standing Committee on Justice and Solicitor General or to such other committees as the House of Commons may consider necessary. Second, it would oversee the activities of the Security Intelligence Review Committee and the Inspector General by reviewing their work plans and reports. Third, it would undertake reviews of a general nature regarding security and intelligence matters that would be of interest to Parliament." [93]

Other parliamentary committees have also reviewed aspects of the security and intelligence community. For example, the House of Commons Standing Committee on Justice and the Solicitor General and the House of Commons Standing Committee on National Defence have each, from time to time, reviewed those security and intelligence activities that fall within their respective mandates. Furthermore, from 1983 to the present, there have been a total of four Senate Special Committees each reviewing aspects of the security and intelligence community.[94]

In addition to these parliamentary reviews, all or part of the security and intelligence community may be, and indeed has been, reviewed by other statutory officers and agencies under various federal statutes. These include the Auditor General, the Privacy Commissioner, the Commissioner of Official Languages, the Information Commissioner, the Canadian Human Rights Commission and, of course, the courts.

For example, in November 1996 the Auditor General prepared and tabled in the House of Commons a report to "inform Parliament about the nature, extent and functioning of the control and accountability arrangements in the intelligence community."[95] When the Auditor General appeared

---

[93] Ibid., p.p. 193-194.

[94] The Senate Special Committee on the Canadian Security Intelligence Service (the "Pitfield Committee", 1983-84), the Senate Special Committee on Terrorism and Public Safety (1986-87), the Senate Special Committee on Terrorism and Public Safety (1989) and this Committee.

[95] Report of the Auditor General for Canada to the House of Commons, Chapter 27: "**The Canadian Intelligence Community - Control and Accountability**". November, 1996.

before this Committee to discuss his report, he advised that it is his normal practice to follow up on audits after a period of two years and that he would be preparing a follow-up report on the Canadian intelligence community for tabling in Parliament in December 1998. In addition, the Information Commissioner conducted an audit of the Communications Security Establishment. In his 1995-1996 Annual Report, he indicated that he was satisfied that the Communications Security Establishment operates in compliance with the *Privacy Act*. He noted that there is no evidence that the Communications Security Establishment intentionally targets Canadians or monitors their communications and added that it uses strict procedures to minimize the possibility that information about Canadians will be inadvertently captured in monitoring foreign communications.

Throughout the hearings, Committee members sought to understand how Canada compares in terms of review or oversight of its security and intelligence community with that of other similar parliamentary democracies. It quickly became clear that there is no single accepted method to review or oversee such organizations.

In the United Kingdom, the Intelligence and Security Committee ("ISC") was established in 1994 to act as a general review body for several of the agencies conducting security and intelligence. However, while this is a committee of parliamentarians, it is not a parliamentary committee. While members are appointed by the Prime Minister, in consultation with the Leader of the Opposition, from sitting members of Parliament, the committee reports to the Prime Minister, not directly to Parliament. The Prime Minister is authorized to deposit reports not dealing with sensitive material before Parliament.

Australia is the only British-style parliamentary system with a standing committee that has review responsibilities for the security intelligence sector. However, it cannot initiate an investigation without parliamentary approval and most significantly, has no mandate to review activities considered to be of a security-sensitive nature. Moreover, the Australian Standing Committee of the House of Representatives on Procedure has, according to testimony to this Committee, recently recommended that the review committee be abolished because of an evident lack of interest.

Several witnesses from the security and intelligence community stated that there is no parliamentary review committee anywhere in the world in any parliamentary system that has anywhere near the access that the Security Intelligence Review Committee has to the Canadian Security Intelligence Service's files and to review of the Canadian Security Intelligence Service's operations.[96] Indeed, the Solicitor General [97] stated that "most of the countries that are doing it [review and oversight] elsewhere are coming to Canada to see how we do it so well."

---

[96] It was not clear from their testimony how widely these witnesses were casting their net in making these statements. It is clear, however, that the United States Congressional oversight committees have at least as much access to information held by the security and intelligence sector as the Security Intelligence Review Committee has to information held by the Canadian Security Intelligence Service.

[97] Andy Scott.

Committee Observations and Recommendations

"Quis custodiet custodes?"
(Who will watch the watchers?)

The security and intelligence community is more open today than ever before and certainly more so than a decade ago. This is particularly the case with the organizations that play a major operational or coordination role in the community, namely the Canadian Security Intelligence Service, the Communications Security Establishment and the Privy Council Office. The Committee also thinks it important to note the existence of a range of review mechanisms currently in place for the community.

The Committee is of the view, however, that there is still some room for improvement. The Committee heard, for example, from the Chairman and the Director of Research of the House of Commons Special Committee that conducted the five year review that their Committee was unable to obtain access to documents that they deemed to be important to the review. Partly as a consequence, they were unable to judge whether the Canadian Security Intelligence Service or its internal or external review bodies were operating properly. Furthermore, what might be called a "special purpose" review body[98] created by statute and with direct linkages to Parliament exists only for the Canadian Security Intelligence Service. Finally, although this Committee heard no evidence that such is currently the case with the Security Intelligence Review Committee or the Communications Security Establishment Commissioner, this Committee is mindful of academic literature that suggests a risk of single purpose review bodies becoming "captured" by the bodies they were established to review. This is said to happen as the review bodies progress from "infancy" through to "maturity" and ultimately to "old age".

The Committee does not see the necessity to establish a permanent parliamentary committee as a special purpose body to review or oversee the Canadian Security Intelligence Service. Nor does the Committee see the need for such a committee to review the Communications Security Establishment specifically if, as this Committee proposes, a permanent "Security Intelligence Review Committee – like" review body is established by statute. It is not necessary and is probably counter-productive to duplicate, even in part, the activities of the Security Intelligence Review Committee and to subject the Canadian Security Intelligence Service and the Communications Security Establishment to another layer of review or a process of continuous review.

Nevertheless, the Committee believes that the nature of security and intelligence demands that there should be a central review body that has the capacity to conduct broad scope reviews of the entire security and intelligence community and individual organizations in it, including "watching the watchers", from time to time. If this central review body is to be an effective counterbalance, it is best located in a different milieu from the existing review bodies and should be completely

---

[98] Contrasting with the general review authorities of the Auditor General, Privacy Commissioner, etc.

independent of Ministers and the Ministry. This Committee recommends that this review body should take the form of a parliamentary committee.

The Committee proposes, therefore, that the Senate establish a standing Senate Committee on Security and Intelligence with a designated chair and membership, in order to ensure reasonable continuity. The Committee would conduct hearings, or otherwise meet, only upon receiving a specific reference from the Senate. In particular, the proposed committee should normally conduct broad scope review of the entire community, rather than specific reviews of individual organizations. In this regard it would be particularly useful for the proposed committee to focus on policies, issues or initiatives that affect the security and intelligence community as a whole and have not been examined by another parliamentary committee.

The proposed committee should also be as forward-looking as possible, helping the government and the security and intelligence community to stay ahead of events. Examples of specific references might include: any legislation pertaining to the Communications Security Establishment, or any other organization within the security and intelligence community; major policy initiatives pertaining to the security and intelligence community that do not fall within the mandate of another Senate committee; and *post facto* reviews of the performance of the security and intelligence in responding to major terrorist incidents or other security offences.

Perhaps the first reference to the proposed Committee could be a study of the need for a review mechanism for the remaining elements of the security and intelligence community and, if a review mechanism is required, the most appropriate mechanism or mechanisms. This Committee also recommends that the proposed Security and Intelligence Committee conduct a broad scope review of the security and intelligence community at least once every five years.

This Committee is concerned at difficulties experienced by previous parliamentary committees in gaining access to information held or generated by the security and intelligence organizations. The oaths of secrecy by Members of the Security Intelligence Review Committee and the Inspector General evidently pose a problem. If the proposed committee is to work, in fact if any parliamentary review mechanism is to work, a solution must be found. It is unreasonable to expect a parliamentary committee to make judgements or determinations based on partial information. It is tempting to insist on Parliament's absolute right to information under Parliament's conventional authority to "send for persons, papers and records". However, experience has demonstrated that, in practice, this power cannot always be effectively exercised, as certainly would prove the case in the security and intelligence field.

Somehow, we have to reach a balance. The balance is between the legitimate requirement of the security and intelligence community to withhold information pertaining to specific operations, targets and intelligence sources; and Parliament's need to know in order to exercise due diligence and accountability.

It is unrealistic to presume that this balance will be achieved overnight. A relationship of mutual trust will have to develop between the proposed committee and the security intelligence community.

If a relationship of trust is to develop, members of the proposed committee must never use sensitive information for partisan or public purposes and the security and intelligence community must not withhold information that the proposed committee has a legitimate need to know in order to perform its mandate.

CHAPTER V

SUMMARY OF RECOMMENDATIONS

1. The Committee recommends that the Privy Council Office maintain a list of terrorist incidents that occur in Canada and those abroad that affect Canadians or Canadian interests. (Chapter I)

2. The Committee recommends that consideration be given to rethinking current definitions of "terrorism", including the definition of "threats to the security of Canada". The Committee suggests a definition that reflects the " gray-zone phenomenon". (Chapter I)

3. The Committee recommends that the Government of Canada continue to work to establish multilateral and bilateral agreements and other international arrangements to counter terrorism and to bring terrorists to justice. (Chapter II)

4. The Committee recommends that the Government of Canada continue to use all legitimate means to influence United States' policy and actions to ensure a common approach and to further the two countries' cooperation and support for each other in the fight against terrorism. (Chapter II)

5. The Committee recommends that the National Counter-Terrorism Plan be signed by each province and that the National Counter-Terrorism Plan constitute the action plan for each province's response to a terrorist incident. (Chapter II)

6. The Committee recommends that where a provincial counter-terrorism plan exists, efforts be made to resolve any conflicts or inconsistencies between that plan and the National Counter-Terrorism Plan. In any event it should be clearly established that in the event of any conflict or inconsistency between the plans, the National Counter-Terrorism Plan shall prevail. (Chapter II)

7. The Committee recommends that the National Counter-Terrorism Plan continue to be regularly reviewed and updated as required, and specifically to address new or emerging technologies that may be used by terrorists. (Chapter II)

8. The Committee urges the Government to ensure that the National Counter-Terrorism Plan be periodically tested through joint training and exercises. (Chapter II)

9. The Committee urges the media and the Government of Canada to continue efforts to develop mutually-accepted guidelines for media conduct during a terrorist incident. (Chapter II)

10. The Committee urges the Government to make the necessary amendments to ensure that the definition of "security exclusion" in the *Immigration Act* and the definition of "threat to the security of Canada" in the *Canadian Security Intelligence Service Act* are in conformity with each other. (Chapter II)

11. The Committee urges the Government to ensure that Citizenship and Immigration Canada receives the technical, personnel and other resources necessary to implement an effective tracing and enforcement system to keep track of refugee claimants within Canada. (Chapter II)

12. The Committee recommends that the Government continue and expand efforts now underway to take concerted action against the smuggling of aliens, using the combined resources of the Royal Canadian Mounted Police, the provincial and local police forces, Customs and Immigration authorities and the United States counterparts of these authorities. (Chapter II)

13. The Committee recommends that consideration be given to amending the *Income Tax Act* to allow Revenue Canada to deny charitable registration to any group on the basis of certificate from the Canadian Security Intelligence Service that the group constitutes a threat to the security of Canada. Any such amendments must be carefully drafted to ensure that the Canadian Security Intelligence Service's decision is adequately reviewed on application by the group, and to avoid a situation where the certificate becomes a bargaining chip in obtaining cooperation from such groups. (Chapter II)

14. The Committee urges the Royal Canadian Mounted Police to retain visibility at international airports in Canada, to serve as an identifier for the travelling public and perhaps also as a deterrent to terrorists and potential criminals. (Chapter II)

15. The Committee recommends that joint counter-terrorist training and exercises be conducted regularly between the Royal Canadian Mounted Police and local police forces, especially those responsible for airport protection and security. (Chapter II)

16. The Committee urges the Government to give immediate and careful attention to the creation of a capability to assess and reduce vulnerabilities in critical infrastructures and to prevent or respond to physical and cyber-attacks. This initiative should involve governments at all levels and the private sector and should address both public and private infrastructures. (Chapter III)

17. The Committee recommends that the Government consider amending the *Criminal Code* to provide specific offences and penalties to deal with cyber-attacks. (Chapter III)

18. The Committee urges the Government, law enforcement agencies and security and intelligence agencies to actively investigate and explore methods and techniques to overcome the policing and security problems posed by emerging encryption technologies. (Chapter III)

19. The Committee recommends that the Canadian Security Intelligence Service, the Communications Security Establishment and the Royal Canadian Mounted Police receive additional resources to acquire the technology and do the work necessary to maintain their current level of access to electronic communications and stored data. The Committee urges Industry Canada to include estimates of these incremental costs for the Canadian Security Intelligence Service, the Communications Security Establishment and the Royal Canadian Mounted Police in the policy proposals that are made to ministers concerning a cryptography policy. (Chapter III)

20. The Committee recommends that the *Criminal Code* be amended to provide lawful access to encryption keys by law enforcement and security and intelligence organizations, and to criminalize the use of encryption in the commission of a crime. (Chapter III)

21. The Committee urges law enforcement agencies, security and intelligence agencies, developers and suppliers of encryption technology and carriers and service providers to consult so that each may better understand the others' requirements and objectives and arrive at mutually-agreed solutions to the problems posed by cryptography. (Chapter III)

22. The Committee recommends that the Government support the training of "first responders" across Canada to identify and respond appropriately to a nuclear, biological or chemical attack, and ensure that they receive the protective and diagnostic equipment they require to respond appropriately to such an attack. (Chapter III)

23. The Committee recommends that a national inventory be established of equipment and other assets available throughout the country to respond to a nuclear, biological or chemical attack. (Chapter III)

24. The Committee recommends that regular joint training exercises to respond to a nuclear, biological or chemical attack be conducted among the Department of National Defence, the Royal Canadian Mounted Police and "first responders" throughout the country. (Chapter III)

25. The Committee recommends that government encourage the proliferation of training and equipping of First Responders on the National Capital model or some enhanced version. (Chapter III)

26. The Committee recommends that steps be taken to ensure that existing mechanisms meet the increasing need and demand for relevant foreign intelligence, including re-examining existing bilateral and multilateral relationships within the current climate and refocusing Canadian foreign service officers and other Canadian employees working abroad to ensure that their information capabilities are working optimally to meet Canada's current needs. (Chapter III)

27. The Committee urges the Government to ensure that adequate and appropriate resources, including policy, financial and personnel resources, be directed to ensure an enhanced strategic orientation to the collection, analysis and production of foreign intelligence. The Committee suggests that this be coordinated and directed by the Privy Council Office. (Chapter III)

28. The Committee recommends that the security and intelligence community explore ways in which parliamentarians may receive regular briefings on security issues and trends, as well as on specific issues for which briefings are requested. (Chapter III)

29. The Committee urges the Royal Canadian Mounted Police and the Canadian Security Intelligence Service to conclude a Memorandum of Understanding to allow the Canadian Security Intelligence Service to have access to the Violent Crime Linkage Analysis System. (Chapter IV)

30. The Committee recommends that the Government examine the feasibility and value of a single security and intelligence "resources envelope" for the coordination of resource allocation within the entire federal security and intelligence community. The Committee further recommends that the Government examine the value of instituting a greater role for the Ministers Meeting on Security and Intelligence in resource allocation. (Chapter IV)

31. The Committee recommends that the mandate and powers of the Communications Security Establishment be set out in an Act of Parliament and that this statute also provides for a permanent review body, separate from but modelled on the Security Intelligence Review Committee, for the Communications Security Establishment. (Chapter IV)

32. The Committee urges the Government to study the feasibility of creating one or more review bodies for the remaining organizations within the federal government's security and intelligence community. (Chapter IV)

33. The Committee recommends that a Standing Senate Committee on Security and Intelligence be constituted, with a designated chair and members, to conduct hearings or otherwise meet only upon receiving a special reference from the Senate. The Committee recommends that the Senate provide references to the proposed Standing Committee to conduct broad scope reviews of the entire security and intelligence community at least once every five years and on policy initiatives pertaining to the security and intelligence community, and *post facto* reviews of the performance of the security and intelligence community in responding to a major incident. (Chapter IV)

APPENDIX A

LIST OF WITNESSES

Tuesday, May 26, 1998

From the Mackenzie Institute:
John Thompson, Executive Director

From the Agassiz Institute for Conflict Studies:
Oliver Peter St. John, Director

As an Individual:
Thomas Quiggin

Tuesday, June 2, 1998

From the University of New Brunswick:
Dr. David Charters, Director, Centre for Conflict Studies

From the Canadian Business Telecommunications Alliance:
Patrick Daley, Executive Director

Monday, June 22, 1998

From the Canadian Bankers' Association:
Ray Protti, President and Chief Executive Officer
Mark S. Weseluck, Vice-President, Banking Operations

From the Bank of Montreal:
Gordon S. Kennedy, Vice-President, Corporate Security
Chairman, Corporate Security Committee

From the Royal Bank of Canada:
Sonny F.E. Saunders, Director, Corporate Security, Head Office

From KPMG Inc.:
Norman Inkster, President, Investigation and Security
Dr. Stephen Schneider, Manager, Investigation and Security

From Transport Canada:

Hal Whiteman, Director General, Security and Emergency Preparedness
Jim Marriott, Security Policy and Legislation

Tuesday, June 23, 1998

From the Ministry of the Solicitor General:

The Hon. Andy Scott, P.C., M.P., Solicitor General of Canada
Jean Fournier, Deputy Solicitor General
James Harlick, Director, Counter Terrorism Division

From the Royal Canadian Mounted Police:

Wayne P. Wawryk, Deputy Commissioner

From the Canadian Security Intelligence Service:

Ward Elcock, Director

Wednesday, June 24, 1998

From the Privy Council Office:

John C. Tait, Senior Advisor to the Privy Council Office and Coordinator of Security and Intelligence
Margaret Ann Purdy, Assistant Secretary to the Cabinet, Security and Intelligence

From the Canadian Security Intelligence Service:

Ward Elcock, Director

From Revenue Canada:

Mark Connolly, Acting Director General, Contraband Intelligence, Services Directorate
Fermo Stefanelli, Director, Intelligence and Operations Division, Services Directorate
George Webb, Manager, Strategic Exports
Stuart McLellan, Senior Intelligence Officer

From the Communications Security Establishment:

Stewart Woolner, Chief
Madeleine Finner, Executive Director

From the Department of Foreign Affairs and International Trade Canada:

Jacques Simard, Director General, Security and Intelligence
H.G. Pardy, Director General, Consular Affairs Bureau

Hugh Adsett, Division of Legal Affairs, Human Rights and Humanitarian Law
Jacques Belac, Director of Physical Security and Staff Protection

From the Department of National Defence:
Lieutenant-General Raymond Crabbe, Deputy Chief of Defence Staff
Colonel Pat Crandall, J2 Operations
Lieutenant-Colonel Don La Carte, Senior Staff Officer, Counter Terrorism and Threat Assessments
Major Bill Reynaert, Director, Nuclear, Biological and Chemical Defence 3-4
Mike Braham, Director, Emergency Programs and Exercises

Thursday, June 25, 1998

From the Ontario Provincial Police:
Detective Chief Superintendent Doug Scott, Bureau Commander, Investigation Support Bureau
Detective Staff Sergeant D.G. Hawkins, Manager, Security Section, Investigation Support Bureau
P. J. Morris, Strategic Intelligence Analyst, Strategic Intelligence Section, Provincial Command Operations

From the London Ontario Police:
Detective Inspector David Lucio, Criminal Investigation Division

From Citizenship and Immigration Canada:
Greg Fyffe, Assistant Deputy Minister, Policy and Program Development
Bill Sheppit, Director General, Case Management Branch
Brian Grant, Acting Director General, Enforcement Branch
Gerry VanKessel, Director General, Refugee Branch

From the Immigration Legislative Review Advisory Group:
Robert Trempe
Susan Davis

Thursday, July 30, 1998

From the Office of the Auditor General of Canada:
L. Denis Desautels, Auditor General of Canada
Henno Moenting, Principal, Results Measurement Audit

From the Senate Protective Services:
Serge Gourgue, Director of Security

From the House of Commons Protective Services:
Michel Thivierge, Director of Security

From the Royal Canadian Mounted Police:
Chief Superintendent Pierre Lange, Protective Operations Branch

Monday, August 17, 1998

From the Office of the Communications Security Establishment Commissioner:
The Hon. Claude Bisson, Commissioner
Joanne Weeks, Commission Secretary

Tuesday, September 1, 1998

From the University of Ottawa:
Professor Ron Crenlinsten, Department of Criminology

From Simon Fraser University:
Professor Stuart Farson

From the House of Commons Committee on Justice and the Solicitor General:
Derek Lee, M.P., Chair, Subcommittee on National Security

From Security Intelligence Review Committee:
The Hon. Paule Gauthier, Chair
The Hon. Bob Rae, Member
Maurice Archdeacon, Executive Director
Maurice Klein, Deputy Executive Director
David Peel, Former Inspector General

From the Office of the Inspector General of CSIS:
Victor E. Gooch, Senior Officer

Wednesday, September 2, 1998

From Industry Canada:
Michelle d'Auray, Executive Director, Electronic Commerce Task Force
Helen McDonald, Director General, Policy Development, Electronic Commerce Task Force

From the Canadian Security Intelligence Service:
Ward Elcock, Director

From the Ministry of the Solicitor General:
Jean Fournier, Deputy Solicitor General

From the Royal Canadian Mounted Police:
Assistant Commissioner Joop Plomp, Dirctor, Technical Services
Chief Superintendent Richard Proulx, Director, Criminal Intelligence Directorate

From the Department of Foreign Affairs and International Trade:
Jacques Simard, Director General, Security and Intelligence
Linda Watson, Director, Export Controls

From the Communications Security Establishment:
Stewart Woolner, Chief

From the Privy Council Office:
Margaret Ann Purdy, Assistant Secretary to the Cabinet, Security and Intelligence

From the Department of National Defence:
Brigadier General Robert Meating, JR Director General Intelligence
Lieutenant-General Raymond Crabbe, Deputy Chief of Defence Staff

As an Individual:
Sam Porteous

Thursday, September 3, 1998

From the Department of National Defence:
Lieutenant Commander Robert Garigue

From the National Capital Region First Responders' Committee:
Lieutenant John Gagnon, Ottawa Fire Department Hazardous Materials Response Team and Chair, NCRRC
Jim Ullett, District Chief; OFD and HMRT Coordinator
Sid McLennan, Firefighter; HMRT Specialist
Sue O'Sullivan, Inspector, Ottawa-Carleton Regional Police Service
Karl Erfle, Inspector, Ottawa-Carleton Regional Police Service
Greg Wilson, Paramedic Officer, Ottawa-Carleton Regional Ambulance Service

From the Ottawa Fire Department:
Gary Richardson, Chief

From the Royal Canadian Mounted Police:
Philip J.M. Murray, Commissioner
Wayne Wawryk, Deputy Commissioner
Giuliano Zacardelli, Deputy Commissioner
Richard Proulx, Chief Superintendent
Tom Quigley, Chief Superintendent

From the Ministry of the Solicitor General:
Jean Fournier, Deputy Solicitor General
Robert Lessor, Director, Counter Terrorism Directorate

From Transport Canada:
Jim Marriott, Director, Security Policy and Legislation

Thursday, October 22, 1998

From the Canadian Security Intelligence Service:
Ward Elcock, Director

Thursday, November 5, 1998

From the National Capital Region First Responders' Committee:
Greg Wilson, Paramedic Officer, Ottawa-Carleton Regional Ambulance Service
Terry Thompson, Captain, Ottawa Fire Department, Hazaradous Materials Response Team, "D" Platoon
John Gagnon, Lieutenant, Ottawa Fire Department, Hazardous Materials Response Team, "C" Platoon Chair

APPENDIX B

LIST OF PEOPLE INTERVIEWED FOR BACKGROUND PURPOSES*

Alfred Prados
Analyst in National Security and Intelligence Oversight Foreign Affairs and National Defense Division Congressional Research Service (United States)

Alan Breakspear
Society for Competitive Intelligence Professionals

Anne Randall
Public Affairs Officer
Australian High Commission (Ottawa)

Anthony Kellett
Defence Analyst
Strategic Analysis Directorate
Department of National Defence

Bill Duhnke
United States Select Committee on Intelligence

Brian Grant
Director General, Enforcement Branch
Citizenship and Immigration Canada

Captain Guy Stevens
Surête du Quebec

Chief Robert Crawford
Emergency Planning
Toronto Fire Department

Dr. Peter Chalk
Lecturer, University of Queensland (Australia)

Dr. S. Shediac
Director, Government Relations and Regulatory Affairs
Sanofi Canada

Dr. David Dewitt
Director Centre for International and Strategic Studies, York University

Dr. Gavin Cameron
Ph.D. Student, St. Andrew's University (Scotland)

Dr. Bob Bach
United States Immigration and Naturalization Service

Dr. Tim Smith
Canadian Security Intelligence Service

Father Francis Xavier

Angela Jendron
First Secretary
Political Information Section
British High Commission (Ottawa)

Chris Williams
United States Deputy Staff Director
Senate Select Committee on Intelligence

David Davidson
Society for Competitive Intelligence Professionals

Detective Steve Irwin
Toronto Regional Police
Intelligence Department

Detective Bob Shirlow
Toronto Regional Police
Intelligence Department

Doug Harrison
Deputy Director
Emergency Measures Ontario

Gerard P. Lynch
Executive Director of Middle Atlantic Great Lakes Organized Crime Link Enforcement Network

Lomar Smith
United States Congressman

Peggy Mason
Canadian Council for International Peace and Security

Pierre Goulet
Acting Director General
Aboriginal Policing Directorate
Solicitor General of Canada

Representatives of United Kingdom Solicitor General

Jim Brown, M.P.P.
Head of Ontario Crime Commission

Richard Viau
Director of Operations Policy,
Planning and Coordination
Directorate of the Health Protection Branch
Health Canada

Representatives of M15 and M16
(London, England)

Brian Beamish
Senior Policy Analyst
Ministry of the Solicitor General of (Ontario)

Thoko Ushe-Robb
Political Clerk
South African High Commission

Jim Wulffe
Director of Security
United States Senate Select Committee

Staff Sergeant Al McIntosh
Peel Regional Police

Ifti Ahmad
Provincial Plans Officer
Emergency Measures Ontario

Tiit Romet
Deputy Chief of Defence
Department of National Defence

**Several persons agreed to meet with Committee staff for background purposes, but asked that their names not be disclosed.*

GLOSSARY OF ACRONYMS AND TERMS

The security and intelligence sector, probably more than any other, seems to use and rely on acronyms and terminolgy that are esoteric. In this Report, the Committee has tried to avoid the use of acronyms. However, for the reader's benefit and to facilitate comprehension the Committee has prepared the following:

Aerobiology Scientific study of the dispersal of infective biological weapons in the air.

AEDPA ***Antiterrorism and Effective Death Penalty Act*** as implemented in 1996 by the United States. It makes providing material support or resources to a designated foreign terrorist organization an offence.

Anthrax Single-celled bacterial organism capable of forming spores. Proves deadly when used as a biological weapon, producing pneumonia-like symptoms.

Bacterium (bacteria) Single-celled microorganism. Most common life form on earth.

BSIS **British Secret Intelligence Service**.

BW Biological Warfare or Weapon Warfare, involves the use of disease usually to kill or debilitate population, food, and livestock.

BWC The Biological Weapons Convention prohibits developing, producing, and stockpiling bacteriological and toxin weapons. Countries must destroy, or divert to peaceful purposes, (not later than nine months after the entry into force of the convention) all agents, toxins, weapons, equipment, and means of delivery. Signed on April 10, 1972, and entered into force on March 26, 1975. Membership includes 124 states. Treaty is of unlimited duration.

CANCERT **Canadian Computer Emergency Response Team** is similar to the United States FedCERT. CANCERT is a private organization that investigates cyber terrorist attacks or network sabotage.

CEIC The Immigration Branch of the Canada Employment and Immigration Commission administers the *Immigration Act, 1976* and Regulations and procedures on the admission of immigrants, refugees and visitors in accordance with he economic, social and cultural interest of Canada.

CIA **Central Intelligence Agency** (United States)
Federal body responsible for the evaluation and dissemination of foreign intelligence within government.

CIC **(Department of) Citizenship and Immigration Canada**

CIS **Commonwealth of Independent States**
The CIS was established in 1991 following the disintegration of the Soviet Union. There are 12 member states: Armenia, Azerbaijan, Belarus,Georgia, Kazakstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.

CISC **Criminal Intelligence Service of Canada**, a division of the RCMP.

CITAC **Computer Investigations and Infrastructure Centre** administered by the Federal Bureau of Investigation.

CIWG **Critical Infrastructure Working Group**

COMINT **Communications Intelligence**

Convention of the Physical Protection of Nuclear Material
Provisions of the Convention oblige parties to ensure that during international transport across their territory or on ships or aircraft under their jurisdiction, nuclear materials for peaceful purposes (plutonium, uranium-235, uranium-233 and irradiated fuel) are protected at the agreed levels. Adopted on March 3, 1980, and entered into force on February 8, 1987. Members include those members EURATOM and 48 other states.

Convention on Nuclear Safety
This Convention is designed to ensure that each member state will review all safety measures of its existing nuclear facilities and, when necessary, make all reasonably practical improvements. If upgrading an installation's safety cannot be achieved, then it should be shut down as soon as possible. Opened for signature on September 20, 1994. Signatories include 54 states, with ratification by one (Norway).

CSE	**Communications Security Establishment**, a branch or division of the Department of National Defence engaged in monitoring and analysing foreign telecommunications for purposes.
CSIS	**Canadian Security Intelligence Service**, set up in 1984 under the Canadian Security Intelligence Service Act.
CW	**Chemical Warfare**
CWC	**The Chemical Warfare Convention** on the prohibition of developing, producing, stockpiling, and using chemical weapons. Also, each state is required to destroy all chemical weapons and chemical weapons production facilities it owns or possesses or that are located in any place under its jurisdiction or control, as well any chemical weapons it abandoned on the territory of another state. The CWC was opened for signature on January 13, 1993. Signatories include 159 states with ratification by 24 states. It enters into force 180 days after the deposit of the 65th instrument of ratification, but not in effect earlier than two years after it was opened for signature.
DFAIT	**Department of Foreign Affairs and International Trade**
DND	**Department of National Defence**
E.I.S.	**Epidemic Intelligence Service** - part of the Center for Disease Control dedicated to investigating outbreaks of disease.
EMINT	**Electronic Intelligence**
ERT	**Emergency Response Team**. ERT's are maintained by most large police forces in Canada to respond to terrorist incidents, hostage takings and other situations involving violence, or the threat of violence.
ESD	**Emergency Services Division** of the Medical Services Branch of Health Canada have training in emergency preparedness and consequence management for major emergencies.
FedCERT	**Federal Computer Emergency Response Team** (United States) acts to counter cyber attacks or network sabotage on critical infrastructures.
FEMA	**Federal Emergency Management Agency** FEMA is a United States federal agency established in 1979 to coordinate responses to terrorist incidents and to provide federal disaster relief. FEMA, along with other federal agencies, provides Weapons of Mass Destruction (WMD) training to State and local first responders.

FIRST **Forum for Incident Response Teams**
FIRST is an international coalition of government and private sector vulnerability analysts and computer incident response teams.

FTO **Foreign Terrorist Organization** as defined by the *United States Antiterrorism and Effective Death Penalty Act.*

GCHQ **General Communications Headquarters** (United Kingdom)

Geneva Protocol - Prohibits the use in war of asphyxiating, poisonous, or other gases, and bans bacteriological methods of warfare. The protocol was signed on June 17, 1925. Membership includes 141 states. Most of the parties in joining the Geneva Protocol made reservations to the effect that they would abide by the terms of the Protocol as long as other states did not resort to the use of CW.

GPS **Global Positioning System**
Constellation of 24 US satellites used to determine precise three-dimensional position anywhere on Earth. Also known as Navstar. Satellites broadcast signals in two forms: encrypted P Code for military use which provides accuracy to within 10m, and Y Code for civil use which provides a horizontal accuracy of 100m and vertical accuracy of 140 m.

H.M.R.U. **Hazardous Material Response Unit**

HEPA **High Efficiency Particle Arrestor**, a type of filter that will trap a virus or a bacterial particle before it enters into the lungs.

HUMINT **Human Source Intelligence**

IAC **Intelligence Assessment Committee**
IAC provides coordination and analytical reports and assessment to the Prime Minister, Ministers and senior officials in government.

IAEA **International Atomic Energy Agency**
Established in 1957 in Vienna, Austria. The United Nations recognized the IAEA as the agency responsible for international activities concerned with the peaceful uses of atomic energy. Membership is 122 states.

IAS **Intelligence Assessment Secretariat**

ICSI **Interdepartmental Committee on Security and Intelligence**
The role of the ICSI is to maintain an overview of security and intelligence issues and provides interdepartmental support to Ministers.

IMINT **Imagery Intelligence**

Inspector General - An official of the Ministry of Solicitor General responsible for the internal review and oversight of the Canadian Security Intelligence Services' activities.

IPAG **Interdepartmental Policy Advisory Group**
IPAG consists of operations, public communications and policy advisory sub-groups and is responsible for preparing Policy and Operation Briefing documents for various officials involved with security and intelligence matters.

IPG **Intelligence Policy Group**
IPG is the principal forum for policy and operational coordination with the security and intelligence community. It is chaired by the Assistant Secretary to the Cabinet, Security and Intelligence and meets bi-weekly.

IPP **Internationally Protected Persons**

IPTF **Infrastructure Protection Task Force**

ISC **Intelligence Service Committee**

JNBCRT **Joint Nuclear, Biological, Chemical ResponseTeam**
JNBCRT is comprised of members from the Canadian Forces and the RCMP to provide a coordinated response to an NBC incident. The Canadian Forces act to aid, assist and assess the terrorist incident, while the RCMP focuses on the disposal, training and investigation of the terrorist threat.

LTTE **Liberation Tigers of Tamil Eelam**

MAGLOCLEN - Middle Atlantic Great Lakes Organized Crime Law Enforcement Network
Established in 1981, it is one of six Regional Information Sharing Systems (RISS) that aids United States and Canadian law enforcement agencies to investigate organized crime, drug trafficking and white-collar crime.

MILINT or MI **Military Intelligence**

Military Hostage Rescue Unit (MHRU)
The MHRU within the Canadian Forces provides armed assistance to the RCMP when requested by the Solicitor General of Canada.

MMSI **Meeting of Ministers on Security and Intelligence**
Chaired by the Prime Minister, members include the ministers whose departments and agencies have primary responsibility for security and intelligence policy and operations.

MOU	**Memorandum of Understanding**
MSG	**Ministry of the Solicitor General**
NACIC	**National Counterintelligence Center** (United States)
NBC	**Nuclear, Biological, and Chemical Weapons**
NCTP	**National Counter-Terrorism Plan**
NEA	**Nuclear Energy Agency** A semi-autonomous body of the Organization for Economic Cooperation and Development, the NEA was established in the late 1950s under the name of the European Nuclear Energy Agency (ENEA) and was renamed the Nuclear Energy Agency in 1972, to reelect its broader membership of non-European countries. Members include Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, Netherlands, Norway, Portugal, Republic of Korea, Spain, Sweden, Switzerland, Turkey, UK and US. Its aims are to promote cooperation between the member governments on the safety and economic progress. The Statute of the NEA contains reference to the objective of preventing the proliferation of nuclear explosive devices, however, the Agency does not have direct nonproliferation responsibilities.
Nerve Agent	A chemical agent that interferes with the central nervous system. This class of chemical weapons agent includes the G- and V-series.
NIPC	**National Infrastructure Protection Centre** is part of the Federal Bureau of Investigation in the United States. Its mandate is to detect, deter, respond to and investigate unlawful intrusions into public or private computer networks.
NOC	**(Royal Canadian Mounted Police) National Operations Centre** The purpose of NOC is to provide support to the Commissioner and senior executive of the RCMP
NSCC	**National Security Coordination Centre**, established to research terrorist incidents in Canada for public knowledge.
NSD	**National Security Directorate** The National Security Directorate is responsible for co-ordinating the federal response to terrorism and identifying priorities for the national counter-terrorism.

Nuclear Non-Proliferation Treaty (NPT)
An agreement to stop the spread of nuclear weapons adopted by the UN General Assembly on June 12, 1968 and signed on July 1, 1968 in London, Moscow, and Washington. Since that time most countries have ratified the treaty, with crucial exceptions such as India, Israel, and Pakistan. In 1995, twenty-five years after the treaty entered into force, it was bated to be extended indefinitely with a review conference every five years.

OECD **Organization for Economic Cooperation and Development**, involves the participation of 53 states from Europe, Central Asia, and North American to act as a political consultative group.

ONA **Office of National Assessments** (Australia)

Organization for the Prohibition of Chemical Weapons (OPCW)
The OPCW comes into being when the CWC enters into force. Headquarter are located in the Hague. Conference of the States Parties is OPCW's principal organ. It is composed of all members of the Organization, to be convened not later than 30 days after the entry into force of the Convention. It will meet annually and in special sessions when necessary.

OSCINT **Open Source Intelligence**

PCO **Privy Council Office**

PIL **Primary Inspection Line**

PLO **Palestinian Liberation Organization**

PMO **Prime Minister's Office**

PSTN **Public Switched Telephone Network**

RCMP **Royal Canadian Mounted Police**

Ricin A plant toxin derived from the coat of the castor bean. Ricin poisoning occurs through blockages of the body's synthesis of proteins.

Sarin One of the G-series of nerve agents. It is composed of methylphosphoryldi-fluoride (DF) plus isopropanol.

SEIT **Security Evaluation and Inspection Team** for the Royal Canadian Mounted Police conducts vulnerability analyses of computer systems for government departments.

SIGINT **Signals Intelligence** (i.e. extracting intelligence from various types of telecommunications)

SIRC **Security Intelligence Review Committee**, the statutory external review body for Canadian Security Intelligence Service.

SJC **Standing Joint Committee for the Scrutiny of Regulations**

STAG **Special Threat Assessment Group** is an interdepartmental committee formed to assess nuclear, biological or chemical threats.

WMD **Weapons of Mass Destruction**

UKUSA Agreement - Agreement between Britain, the United States, Australia, Canada and New Zealand setting out inter alia, the responsibilities of these nations for monitoring Soviet communications and sharing signals intelligence.